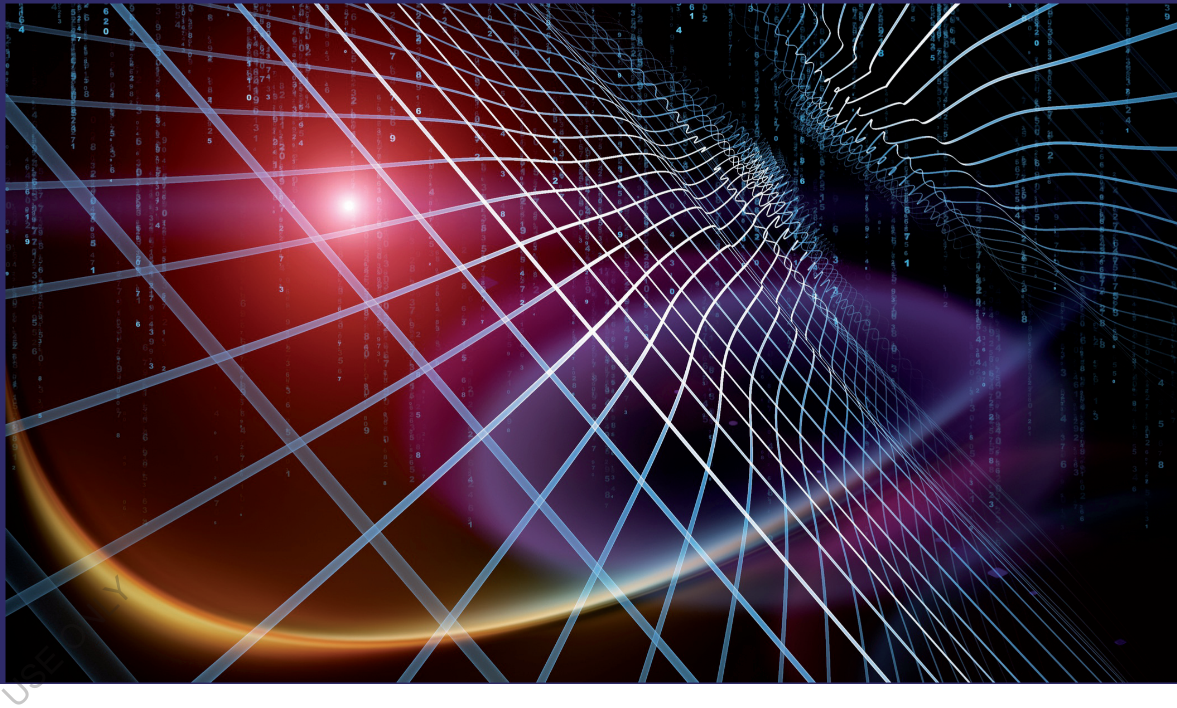
Security is one of the most important problems that have attracted a lot of research and development efforts in the past few years. In multi-hop wireless, ad-hoc network path error and malicious packet dropping are two major resources for packet losses. The packet losses are caused by connection errors and malicious drop are to be recognized by observing a sequence of packet losses in the network. The insider-attack case malicious nodes that are part of the route exploit their knowledge of the communication in the network. The malicious node drops a large amount of packet losses critical to the network performance. The research study observing the dynamic packet dropping rates in the wireless network. The rate is comparable to the control error rates that are based on distributed manner. The proposed research work presents a new approach to measure the dynamic privacy preserving in wireless networks using the methodologies namely, Network Model, Network Routing Model, Privacy Preserving Link State Routing Protocol and Dynamic Non-linear authentificator Protocol algorithm (DNAP). The Path Detection (PD) protocol used to find the alternate path to transfer a message to destination.



Dr. B. Radha has done her PhD in Computer Science from Anna University in 2015 on Resource Selection and Scheduling in Grid. She did MCA Degree in 2004 and B.Sc Degree in Chemistry in 2001. She is currently working as an Associate Professor in the Department of Information Technology, Sri Krishna College of Arts and Science, Coimbatore.

978-620-0-27827-2

Radha Balasubramanian (Ed.)
R Jayaprakash
B Iswarya

A Complete Guide for Cluster Based Network

LAP LAMBERT Academic Publishing

Radha Balasubramanian (Ed.)
R Jayaprakash
B Iswarya

A Complete Guide for Cluster Based Network

Radha Balasubramanian (Ed.)
R Jayaprakash
B Iswarya

A Complete Guide for Cluster Based Network

LAP LAMBERT Academic Publishing

Cover image: www.ingimage.com

Publisher:
LAP LAMBERT Academic Publishing
is a trademark of
International Book Market Service Ltd., member of OmniScriptum Publishing Group
17 Meldrum Street, Beau Bassin 71504, Mauritius

Printed at: see last page
ISBN: 978-620-0-27827-2

A Complete Guide for Cluster Based Network

Table of contents

Chapter - 01

Network: An Introduction

A network is defined as a group of two or more nodes or computer systems linked together to the share the information with each other.

Cluster Network

A computer **cluster** is a set of loosely or tightly connected computers that work together and they can be viewed as a single system.

Types of Network

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose.

Some of the different networks based on size are:

- Personal area network, or PAN
- Local area network, or LAN
- Metropolitan area network, or MAN
- Wide area network, or WAN

Characteristics of network

These following types of network characteristics also used to categorize the types of network.

Network topology: Network topology is the geometric arrangement of computer systems. In practically highly used topology are Bus topology, Star topology, Ring topology, mesh topology etc.

Network Protocol: A Network protocol defines a common set of rules and signals for computer systems on the network use to communication. Highly preferred network protocol in real time environment is LAN, sometimes called Ethernet. Another popular LAN protocol for personal computers is the IBM token-ring network.

Network Architecture: Network architecture can be broadly classified as using either a peer-to-peer or client/server architecture.

Additional Characteristics

- **Sharing Resources** from one Computer to another Computer over a network
- **Performance** by measuring the speed of data transmission with number of users, connectivity and the software used
- **Reliability** makes easy to use an alternative source for data communication in case of hardware failure or connectivity issues
- **Scalability** increases the system performance by adding more processors
- **Security** is the main characteristics of Computer network where you can take necessary steps for protecting your data from unauthorized access

Network Goals

- The main goal of networking is "Resource sharing", and it is to make all programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user.
- A second goal is to provide high reliability by having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable, the other copies could be available.
- Another goal is saving money. Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more. This imbalance has caused many system designers to build systems consisting of powerful personal computers, one per user, with data kept on one or more shared file server machines. This goal leads to networks with many computers located in the same building. Such a network is called a LAN (local area network).
- Another closely related goal is to increase the systems performance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.
- Computer networks provide a powerful communication medium. A file that was updated or modified on a network can be seen by the other users on the network immediately.

Chapter - 02

Network Basics

NETWORK APPLICATIONS

- Access to remote programs.

- Access to remote databases.
- Value-added communication facilities.

Ad hoc Network

An **ad hoc network** is a type of temporary computer-to-computer connection. In **ad hoc** mode, you can set up a wireless connection directly to another computer without having to connect to a Wi-Fi access point or router.

Client-server is a relationship in which one program (the client) requests a service or resource from another program (the server). At the turn of the last century, the label client-server was used to distinguish distributed computing by personal computers (PCs) from the monolithic, centralized computing model used by mainframes.

Today, computer transactions in which the server fulfills a request made by a client are very common and the client-server model has become one of the central ideas of network computing. In this context, the client establishes a connection to the server over a local area network (LAN) or wide-area network (WAN), such as the Internet. Once the server has fulfilled the client's request, the connection is terminated. Because multiple client programs share the services of the same server program, a special server called a daemon may be activated just to await client requests.

In the early days of the internet, the majority of network traffic was between remote clients requesting web content and the data center servers that provided the content. This traffic pattern is referred to as north-south traffic. Today, with the maturity of virtualization and cloud computing, network traffic is more likely to be server-to-server, a pattern known as east-west traffic. This, in turn, has changed administrator focus from a centralized security model designed to protect the network perimeter to a decentralized security model that focuses more on controlling individual user access to services and data, and auditing their behavior to ensure compliance with policies and regulations.

Advantages and disadvantages of the client-server model

An important advantage of the client-server model is that its centralized architecture helps make it easier to protect data with access controls that are enforced by security policies. Also, it doesn't matter if the clients and the server are built on the same operating system because data is transferred through client-server protocols that are platform-agnostic.

An important disadvantage of the client-server model is that if too many clients simultaneously request data from the server, it may get overloaded. In addition to causing network congestion, too many requests may result in a denial of service.

Client-server protocols

Clients typically communicate with servers by using the TCP/IP protocol suite. TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control and handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. In the Open Systems Interconnection (OSI) communication model, TCP covers parts of Layer 4, the Transport Layer, and parts of Layer 5, the Session Layer.

In contrast, IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

Other program relationship models

Other program relationship models included master/slave and peer-to-peer (P2P). In the P2P model, each node in the network can function as both a server and a client. In the master/slave model, one device or process (known as the master) controls one or more other devices or processes (known as *slaves*). Once the master/slave relationship is established, the direction of control is always one way, from the master to the slave.

Chapter - 03

CBPPRS: CLUSTER BASED PRIVACY PRESERVING ROUTING SELECTION IN WIRELESS NETWORKS

Abstract

In wireless mobile ad hoc network, each node / junction is proficient of transfer message (information) with dynamism without constraint of any permanent infrastructure environment. Movable nodes commonly progress inside or outside from the entire network dynamically, building network topology unbalanced in mobile ad-hoc network (MANET). In a privacy preserving network group, cluster head is dependable for communication with associates in a cluster which consumes additional battery (energy) supremacy in evaluation to cluster members in a cluster. As a message transmission inside and outside cluster as a result, it becomes an enormously testing job to maintain stability in network. In this paper aims to present a cluster based privacy preserving routing protocol selection algorithm in inside and outside cluster using NS (Network Simulator) 2.34 Framework. The proposed routing protocol selection based Cluster head selection formation operates exclusively based on source routing and on-demand process, it has been selected as the routing protocol to be executed and tested for ad hoc network application characterized by a source on-demand message conversation between nodes in a portable ad hoc network

Keywords: *Cluster, Cluster Head, Gateway, Privacy Preserving, Wireless Networks.*

1. INTRODUCTION

A MANET (Mobile Ad hoc Network) consists of an amount of mobile nodes equipped among a transmitter and a receiver. MANET was envisioned to generate a network dynamically on-the-fly without relying on any wired infrastructure. That is why; they are besides called “communications less network”. Unlike the infrastructure-based networks such as a cellular network, all the components of an ad hoc network are highly mobile and outstanding to this mobility, the topology of the network changes dynamically (Jayaprakash et al., 2017). The base station in cellular networks is analogous to the cluster head in ad hoc networks; however, the difference is that base stations are stationary while the cluster head themselves are also mobile. Fixed wireless networks usually exist in a form of a master slave relationship. However, MANETs do not share this characteristic. Nodes rely solely on each other to established communication links and act as routers to convey data packets between source and destination pairs. Since the data packet may need to travel from a starting node (source) to a target node (destination) through a cluster of intermediate nodes, yet another name for ad hoc networks is “multi-hop networks”.

Clustering is the progression of separating the network into interconnected substructures, named clusters (S Pathak et al., 2014). In a clustered network, nodes are divided into distinct logical set (clusters), which is allocated geographically adjacent to each other. A distinctive cluster structure is revealed in Figure 1.

As depicted, nodes are divided into logic groups (within the dotted lines) according to the rules of the clustering scheme. “Nodes may be assigned a different role or function, such as cluster head, gateway or cluster member (M Chatterjee et al., 2004) & (P Jianli et al., 2008). A cluster head typically serves as a coordinator for its cluster, performing intra-cluster management functions and data-forwarding”.

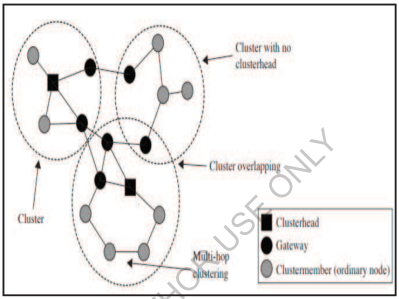


Figure 1. Structure of the cluster

A gateway is a node with inter-group mechanism links, which can forward information between clusters. There are clustering schemes that support cluster overlapping. In other words, two distinct clusters may share nodes. In this case, gateway nodes may be assigned to more than one cluster. Finally, cluster members, also referred as ordinary nodes, do not possess special cluster maintenance functions; they simply belong to a cluster.

A clustered (group) topology in large network enables efficient performance. The cluster structure provides several benefits, some of which mentioned below.

1.1 Reduced Topology Information

Due to the number of nodes or junctions inside of a cluster being lesser than the number of nodes of the whole network, the clustering process eases the aggregation of topology information. As a result, each node required to stock up a reduced portion of the complete network routing in rank.

1.2 Routing Efficiency

In a flat architecture all node bears identical responsibility to proceed as a router for forwarding packets. The great amount of message flooding inherent to path discovery reduces the routing efficiency (W Bednarczyket al., 2013). A clustered structure improves routing efficiency and makes the path discovery easier.

1.3 Efficiency and Stability

In the perspective of a mobile node, the network appears smaller. Thus, when a mobile node disconnects or switches to another cluster, only the nodes residing in the corresponding clusters are required to vary their fact structures. There are further advantages that are transversal to the mentioned benefits. As a product of clustering, the communication bandwidth, energy consumption, throughput and scalability are improved.

The aim of this work is to develop a cluster based privacy preserving routing protocol in MANET framework is to effectively partitioning inside and outside cluster message transmission in secure manner. In this paper, we will discuss the routing process of routing topology deployment and initial cluster head formation in privacy manner.

The rest of the paper is ordered as follows: Literature Review detailed is in Section 2, Section 3 - Cluster formation process and conclusion in Section 4 respectively.

2. Literature Review

(W You et al., 2015) proposed that the end-to-end model, which was calculated for individual data transmission in the before time period of Internet, is reasoning difficulties universally in currently content based web services. Accordingly, Information Centric Network (ICN) is projected to resolve these problems. As the majority permanent clean-slate advance for subsequently generation Internet, ICN has concerned greatly consideration from network researchers in the past little years. This review focused on the present development of the research work in ICN. It examined different key features such as naming and routing systems, in-network caching strategies, etc., and highlights the advantage of implementing ICN, open research problems and new interests in this domain.

(M Ulema, JM Nogueira, B Kozbe, 2006) projected that "A wireless sensor network consists of great information of sensors, which are tiny, low-cost, low-power radio procedure committed to performing confident functions such as gathering different ecological data and transfer them to communications processing channel nodes. The field of wireless sensor networking is too in advance better interest among not just researchers but also mixed groups such as environmental, public security, military and medicine. This tutorial creates with a summary of the wireless sensor networks. An assessment of the present technologies used for these types of wireless methods of network. The focus is on the architectural concern such as routing, topology and protocols. Lastly, the network executive issues connected to wireless sensor networks are discussed. The tutorial concludes with a conversation of the open research problems in this area."

(C Suchismita & R Santanu Kumar 2009) projected “Single-hop clustering method accepts the simple system to create the rational panel of the dynamic network where the network topology modifies continuously resultant an unbalanced clustering. In this paper creates a complete survey of various bench-mark single-hop clustering algorithms to recognize the research developments in this area. The literature presents the logic of cluster formation for special algorithms in completes linked cluster architecture and an exhaustive simulation review of their performance on the cluster protection features such as frequency of cluster reelection, cluster density, frequency of cluster modifies by the mobile nodes and the granularity of cluster heads. This paper must assist the researchers as well as practitioners in preferring an appropriate clustering algorithm on the source of their configuration and maintenance overhead, prior to every routing method be accepted in the mobile ad hoc network.”

(JY Yu & PHJ Chong 2005) discovered that “Clustering is a significant research subject for portable ad hoc networks (MANETs) since clustering creates it promising to assure a basic level of system presentation, such as accuracy and delay, in the occasion of mobility and a huge number of mobile terminals. A huge variety of approaches for ad hoc clustering have been obtainable, whereby special approaches normally focus on different performance metrics. This article presented a complete review of recently proposed clustering algorithms, which to classify based on their ideas. This survey provides descriptions of the methods, evaluations of their performance and rate, and discussions of advantages and disadvantages of every clustering method. With this item, readers can have an additional through and fragile accepting of ad hoc clustering and the research developments in this area.”

(J-H Ryu et al., 2001) stated that “Distributed heuristic clustering methods are proposed that reduce the necessary broadcast power in two-tiered mobile ad hoc networks. Both methods can be realizing and executed in real time and can be assumed for periodic or event-driven cluster reconfiguration. Method presentation is simulated and evaluated with optimum configurations based on the signify spread power and the describe drop velocity as performance measures.”

(A Ephremides et al., 1987) future that “Network survivability is attained during the use of scattered network control and rate of recurrence hopping spread-spectrum indicating. The authors demonstrated how the implementation of the completely distributed Linked Cluster Algorithm can allow a network to reconfigure itself when it is concerned by connectivity modifications such as that resultant from jamming. Further resistance besides jamming is presented by frequency hopping, which directs naturally to the use of code division multiple access (CDMA) methods that allow the simultaneous successful transmission by some users. Distributed algorithms that develop CDMA belongings have been developed to plan contention-free transmissions for greatly of the channel access in this network. Contention-based channel access protocols can also be executed in conjunction with the Linked Cluster network configuration. The design concept obtainable in this paper provides a high amount of survivability and flexibility, to contain changing environmental circumstances and user strain.”

(CH Liu et al., 2015) designed that “Energy control in a digital handset is basically implemented in a separate fashion, and frequently, such a Discrete Power Control (DPC) system is suboptimal. In this paper, authors illustrated initial show that in a Poison-distributed ad hoc network, if DPC is correctly considered with a confident condition satisfied, it can strictly work improved than no power control (i.e., users employ the same constant power) in conditions of standard signal-to-interference ratio, outage chance, and spatial reuse. This ideology indicates us to have an N-layer of DPC design proposal in a wireless mobile clustered ad hoc network, where source and receivers in globular clusters are distinguish by a Poisson cluster process on the surface. The cluster of every transmitter is tessellated into N-layer annuli with transmit power Pi accepted if the intended receiver is positioned at the i^{th} - layer."

(F Al-Kalani et al., 2008) proposed that "In mobile network, the clustering method varied due to the mobility of the mobile nodes some time in any direction. That reasons the separations of the network or the combination of mobile nodes. Some presented centralized or globalized algorithm have been proposed for clustering method, in a way that no single node becomes remote and no cluster becomes congested. A particular node called head cluster or organizer is chosen, has the position to arrange the distribution of nodes in clusters. The authors proposed a spread clustering and head (leader) selection mechanism for Ad-Hoc mobile networks, in which the head is a mobile node. The experimental results demonstrate that, in the case of leader mobility the time required to choose a new leader is less significant than the time desirable an important topological modify in the network is occurs."

(R Pandi Selvam et al., 2011) stated that "In ad-hoc networks, clustering is a significant and recognizable method to separate the huge network into some sub networks. According to the dynamic topology the clustering is believes as complex process in ad hoc networks. In this paper, they have determined to plan a new value based clustering algorithm to progress the presentation in this wireless communication technology. Execution experiments are performed to review the effective performance of the algorithm in the broadcast range, quantity of mobile nodes and maximum displacement."

(C Chiang et.al, 1997) noted that "A cluster head-token communications for multi-hop, mobile wireless networks has been considered. Conventional routing algorithms in wire line networks are not reasonable for transportable wireless environment right to the active change in link connectivity. To increase the superior performance for clustered multi-hop, mobile wireless networks, routing should take into account radio channel access, channel reservation and code forecast. In this paper, authors proposed various heuristic routing methods for clustered multi-hop, mobile wireless networks. A message delay development up to four fold has been experimental in the simulations evaluated with shortest-path method, making multimedia traffic feasible. A means of communication channel structure has been incorporated on the way to examine the impact of channel fading on the protocols."

(Jayaprakash R & Radha B 2017) quoted that CBPR in Mobile network using Privacy Preservation manner including inside and outside cluster has provided new direction for to develop and improved techniques for wireless ad-hoc network.

3.CLUSTER FORMATIION ROTUING PROCESS

The cluster formation in privacy preserving routing process considers the clustering network region is alienated on several polygons, each called a cluster. All clusters have a center with coordinates defined as cluster location that could be used as cluster identity (ID). A node close to the cluster center is chosen as cluster head (CH). CH directs the positions of nodes fit in to that cluster. While moving inside a cluster, a node requests to broadcast its position only to the nodes that reside in that cluster. A node's cluster location is simplified when it leaves its own cluster and goes into an additional cluster. "Cluster based routing is performed by using two steps. The initial pace is inclusive dynamic routing in which messages are moved from individual group to a different group that is nearer to the target depending on cluster locations. Communications are promoted based on right-hand strategy in case of dead end cluster. The next step is called privacy preserving cluster based steering in which datagram's are routed connecting clusters". The figure 2 describes the cluster based privacy preserving routing protocol flow.

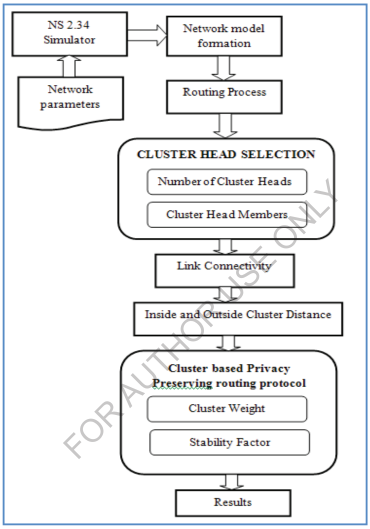


Figure 2. Cluster based privacy preserving routing protocol flow

3.1 Network Formation

In network formation process is evaluated in graph formation. As a graph denoted as $G = (N, L)$, where N represents the set of mobile nodes and L represents the group of Links/lines/edges among the nodes. In this model consists of n amount of heterogeneous mobile nodes randomly arranged in the simulation tool environment. Every node has the unique identity (ID) and is prepared with Omni-directional projection. It is implicit that nodes are position alert and can compute their qualified distance to their neighboring nodes. Let $P_{max}(k)$ be the maximum transmission power, let $P_{min}(k)$ be the minimum transmission power, and let P_k be the transmission power of a mobile node $k \in L$. To begin with mobile nodes broadcast with maximum power P_{max}.

In this proposed scheme the network formation is assumed that transmission power (k) can be regulated linking the maximum and minimum value; that is, $P_{min}(k) \leq P(k) \leq P_{max}(k)$. Let P_{kv} be the minimum transmission power essential to communicate between nodes k and v, which can be calculated as $P_{kv} = Dist^{\beta} + C$, where $Dist$ is the Euclidean remoteness between k and v, β is the path loss exponent, where $2 \leq \beta \leq 4$, and C is a constant value. Let Graph $G = (N, L)$ be a primary topology of the network and let $G' = (N, L')$ be the topology, achieved when the transmission power control method is applied at mobile nodes.

3.2 Routing Process

The routing process is completely based on-demand of ad hoc network routing protocol composed of two parts: Route Discovery (Identity) and Route Maintenance (Preservation).

- Route Discovery is mainly used to search (find) a path; this node is known as the originator of the Route Discovery, and the destination of the message is recognized as the Discovery's object.
- Route Maintenance is the method by which the node conveys a message alongside a particular path to various destinations identifies if that path has broken down, for example since two nodes in it have stimulated moreover separately.

Routing process in mobility clustering is complicated as an end product of the self motivated environment of association topology and their resource conditions. The problem of connection consistency in mobile ad hoc networks is a major concern to broadcast packets throughout network layouts. Direction-finding process in multi-hop wireless networks via the shortest-path process is not relevant situation to build fine superiority routes, because least amount hop count routing frequently selects paths that have extensively a lesser amount of capacity than the finest routes in the network.

3.3 Cluster Based Privacy Preserving Routing Selection

The cluster head selection is attractive that a cluster head has the highest number of single-hop neighbor's node within its broadcast range and least amount rate of nodes moving away of its communication range. "Since during Cluster Head formation/reformation, it is not easy to compute the number of junctions moving into present neighborhood group in later and their leave-taking rate after moving in. As a result, just the number of available junctions within the current cluster is considered at that time of Cluster Head setting up or else updating. The proposed method demonstrate the amount of single-hop neighbors when conducting the cluster creation/recreation as *N* and the rate of nodes leaving as *v* Maximizing *N* can decrease the average number of clusters in the network, which can save energy and reduce the rate of associate member interchanges between various cluster groups. Minimizing *N* results in the links connecting a cluster head and the cluster elements to be high stable". In other words, the cluster construction is more resilient to the moment of nodes, which can decrease the number of manage packet transparency, enhance the routing constancy and diminish the broadcast delay.

Cluster Based Privacy Preserving Routing Selection considers the collection of Cluster heads (CH) in a mobile ado network of *n* junctions/nodes such that all nodes in this network are within distance *h* hops of a *CH*, for a known DEFINED - VALUE. In the proposed CHS representation flow described in figure 3, the Cluster duration indicates the instance from the position of node is chosen as Cluster head until the position of a node modifies its condition to standard node. It should be noted that the Cluster generation is needy on mobility problems; the Cluster duration in stable network depends on link reliability. In the simulation model (using NS2.34 Tool) a Clustering packets is sent every 2 seconds. Thus, a neighbor node is reserved in the neighbor table for $2 * CNT\ R$ seconds and discarded if there is no additional Clustering communication received. Primarily, the Statement History (SH) for all mobile nodes has been calculated as empty or ≥ 1. Algorithm 1 represents the Cluster head(s) identifying progress as well as a flow diagram has been revealed in figure 3.

From equation (1) DEFINE - VALUE can be further calculated by;

$$DV_{ij} = \frac{\sum_{n=i}^{m} DV_{ij}}{SH} \qquad eqn.(1)$$

Where $i, j \in$ mobile nodes (points); DV_{ij} is node *i*'s DEFINED - VALUE for node/junction j. Appropriate lively changes in the topology of system, the Cluster (group) formation is indentified from every time to time.

Algorithm 1: CLUSTER BASED PRIVACY PRESERVING ROUTING SELECTION

```
Initialize $CH_{cur} \leftarrow 0$; $CH_{prev} \leftarrow 0$; $Time_{prev} \leftarrow 0$; $Current() \leftarrow 0$;
Step 1: Time – $OUT_{loop} \leftarrow 2$
Step 2: equation (1) DEFINED-VALUE can be further evaluated
```

```
    $D_{nij}(t_2) = D_{nij}(t_1) * \exp[-(D_{nij}(t_1)\Delta t)]^{2k}$
    Where $\Delta t = t_2 - t_1$ and $k$ is an int value, i.e. $k \geq 1$
Step 3: while $Time_{prev} \leq Current()$|| DEFINE – VALUE($CH_{prev}$) $\leq 1$ = true do
    $CH_{prev}$ remains as Cluster head
    End while
Step 4: if DEFINE – VALUE($CH_{prev}$) = DEFINE – VALUE($CH_{cur}$) && $SH(CH_{pre})$ = SH($CH_{cur}$) then
    Both $CH_{prev}$ and $CH_{cur}$ stay as cluster heads
    Else
    Choose latest Cluster (group) Heads
    End if
```

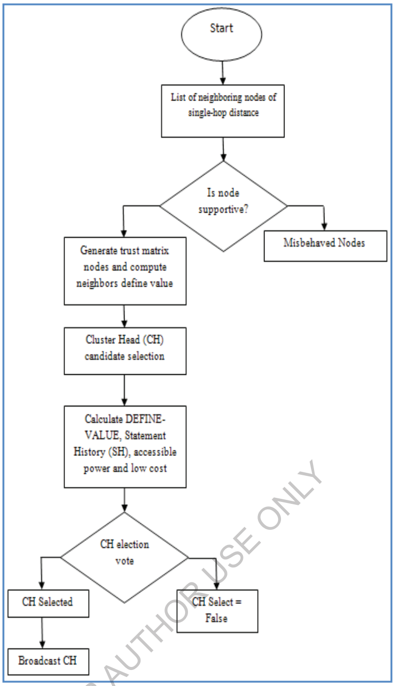

Start
List of neighboring nodes of single-hop distance
Is node supportive?
Misbehaved Nodes
Generate trust matrix nodes and compute neighbors define value
Cluster Head (CH) candidate selection
Calculate DEFINE-VALUE, Statement History (SH), accessible power and low cost
CH election vote
CH Selected
CH Select = False
Broadcast CH

Figure 3. Flow diagram - To identify the cluster head

Table 1

The simulation representation considers 51 nodes in Cluster Based Privacy Preserving Routing Selection network, with nodes (vertex) randomly deployed in a 300 m x 300 m simulation area. The simulation parameters is given below,

Parameters	**Symbol**	**Value**
Mobile Nodes	MN	5-50 in steps of 10
Simulation Area	Width x Column	300 x 300
Transmission Range	TR	5-50 in steps of 10
Distributed Weights	D_{w1}, D_{w2}, D_{w3}, …, D_{wn}	(0.1, 0.04, 0.05, 0.2, 0.5)
Node Energy	E_{node}	100Joules
Boosting Energy	E_{boost}	100J/bit/m^2

4. Conclusion

In this paper reviewed and analyzed the cluster based privacy preserving routing selection methodology algorithm for portable ad hoc networks on the strength of linkage and cluster head selection formation. Necessary factors such as node speed, relative energy of the node, remaining energy and weights are well-thought-out to establish an appropriate clustering inform period and choose head of cluster. To make a substitution among the corresponding issues with no weights combination needed, this paper proposed a cluster weight in privacy preserving manner routing protocol selection algorithm for cluster head selection technique. These constraints are used to progress and enhanced cluster head constancy, cutback in the amount of clusters in the network, and civilizing the energy effectiveness. Meanwhile, the proposed system build a link generation methodology to calculate approximately the generation of every connection and proposed a highest group head revised space (edges generation) representation to recognize the grouping update occurrence.

References

[1] Bednarczyk W, P Gajewskil. (2013). An enhanced algorithm for MANET clustering based on weighted parameters. Universal J. Commun. Netw. 1(3), 88–94.

[2] Chatterjee M, SK Das, D Turgut. (2002). WCA: a weighted clustering algorithm for mobile ad hoc networks. Clust. Comput. 5, 193–206 Kluwer Adademic Publishers, Manufactured in The Netherlands.

[3] Chiang C, H. K Wu, W Liu, & M Gerla. (1997). Routing in clustered multihop, mobile wireless networks with fading channel. Proceedings on IEEE SICON'97. pp. 197–211.

[4] Ephremides, Jeffery Wieselthier, Dennis Baker. (1987). A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling. Proceedings of the IEEE Vol 75,No. 1, pp. 56-72.

[5] Jayaprakash R, Radha B. (2017). Routing Protocols and Privacy Preserving Cluster Based Protocols in Wireless Networks : A Technical Review. International Journal of Advance Research in Science and Engineering (IJARSE), Vol 6, No.12. pp.1325-1333. http://www.ijarse.com/images/fullpdf/1514011896_867ijarse.pdf

[6] Jianl Pi. R Jain. (2008). A survey of network simulation tools: current status and future developments.

[7] Liu CH, B Rong, S Cui. (2015). Optimal discrete power control in poisson-clustered ad hoc networks. IEEE Trans. Wirel. Commun. 14(1), 138–151.

[8] Pandi Selvam R et al., (2011). Stable and flexible weight based clustering algorithm in mobile ad hoc networks. Int. J. Comput. Sci. Inf. Technol 2(2), 824–828.

[9] Pathak S, N Dutta, S Jain. (2014). An improved cluster maintenance scheme for mobile adhoc networks, Advances in Computing, Communications and Informatics (ICACCI, IEEE-International Conference), Pp.2117-2121.

[10] Ryu J-H, S Song, D-H Cho. (2001). New clustering schemes for energy conservation in two-tiered mobile ad-hoc networks. Proc. IEEE ICC\'01 3, 862–866.

[11] Suchismita C, R Santanu Kumar. (2009). A survey on one-hop clustering algorithms in mobile ad hoc networks. J. Netw. Syst. Manag. 17, 183–207.

[12] Ulema M, JM Nogueira, B Kozbe. (2006). Management of wireless ad hoc networks and wireless sensor networks. J. Netw. Syst. Manag. 14(3), 327–333.

[13] Vasilakos AV, Z Li, G Simon, W You. (2015). Information centric network: research challenges and opportunities. J. Netw. Comput. Appl. 52, 1–10 Elsevier Ltd.

[14] Yu JY, PHJ Chong. (2005). A survey of clustering schemes for mobile ad hoc networks. IEEE Commun. Surv. Tutorials 7(1), 32–48.

[15] Zabian, A Ibrahim, F Al-Kalani. (2008). Dynamic head cluster election algorithm for clustered ad-hoc networks. J. Comput. Sci. 4(1), 42–50.

Chapter - 04

LOAD HARMONIZING ARCHITECTURAL DESIGN SCHEME FOR CBPR NETWORKS

Abstract: Weight Pondering is a fundamental constraint of several multi-hop wireless technologies. A cluster based direction-finding procedure is work on its potential to share out transfer in excess of the systems mobile nodes and a superior direction-finding etiquette realizes this devoid of establishing intolerable hold-up. In generally understandable benefit is visible in escalating the life of battery (energy) occupation mobile node which can ultimately improve the permanence of the whole arrangement. This paper presents a original work of evaluation the load based on solitude (privacy) routing (direction finding) protocol (LBCPR) algorithm for mobile commercial networks on the power of relationship and head of the cluster selection construction with help of NS 2.34 construction. LBCPR load disproportion in the group and the preconception or favouritism in preference up centrally situated points for data passing. The anticipated cluster based direction finding metric, weight and a minimal principle en route for make a decision to the pathway that occupies mobile nodes by way of fewer weight on them. Besides, it is revealed that LBCPR procedure ropes a hard faithfulness is expand in conditions of through performance put grades which give you an idea about an evidence of theory for weight pondering properties of the planned premise.

Keywords: Cluster, Load Balancing, Gateway, Privacy Preserving, Wireless-Networks.

1. Introduction

"Transportable networks (MANET) are sovereign systems shaped by number of movable points exclusive of several announcement supports". Path finding in MANET is somewhat difficult because of its vibrant situation of the association framework. Even though frequent direction-finding protocols have been designed for MANETs, such as Destination Sequence Distance Vector and AODV, these path finding protocols are not fitting for vast MANET for the reason that the lucidity for protecting state-of-the-art routing in sequence at every node rapidly becomes undesirable as network dimension increases. Clustering is systems that separation a network into special groups or clusters, generating a sensible hierarchy in the system. By screening a set of connections into disparate clusters, announcement overheads for preserving up-to-date routing information can be extensively reduced. Conversely, clustering still deserves overhead that has yet to be examined in depth.

Control visual projection is a considerable evaluate for computing act [10] mechanism of grouping because bandwidth is a curtailed and high-priced resource in MANETs (*Chatterjee M*, *SK*

Das, *D Turgut*, *2002*).

As system facet increases utilization of bandwidth becomes more significant feature that involves general recital of a set-up. Above the precedent hardly any years, frequent cluster systems encompass been projected. Nevertheless reserved idea of analysing on cluster overhead is tranquil missing. The mainstream of previous job on clustering visual projection focus on the proclamation and time convolution of an algorithm is a patchy ballpark figure of grouping of clouds with worth to network dimension.

2. Clustering scheme in MANET

Clustering scheme, [9] an indispensable research focus on mobile system called MANETs because it creates feasible to assurance critical steps for scheme recital, such as concert and setback, occasion to both moment along with a massive quantity of transferable workstations. An enormous series of methods for ad hoc clustering have been vacant, whereby diverse methods on whole spotlight taking place diverse concert metrics. Dynamic course-plotting is in region key concern of MANET. Though, it has been established that a level formation entirely on method of pro-active or re-active routing methods can't attain glowing in an enormous lively MANET [11] (*Chiang C*, et.al., *1997*). In erstwhile words, an even arrangement meets scalability problems with enlarged set-up dimension, particularly in countenance of bump moment at similar (same) instance. This method is suitable for fundamental uniqueness. The announcement of transparency path-based pro-active steering enlarges with the quadrangle amount transportable nodes. An imprudent course-plotting method, disquieting R-REQ broadcasting in excess of entire set-up, substantial path group setback turn to impossible in attendance of equally a huge amount of portability. Therefore, a hierarchical structural design is necessary for achieving an elementary recital promise in a great dimension to network.

Classic huddle framework is shown in Fig. 1. From that we can get idea of mobile nodes are estranged in an amount of effectual groups/cluster (with scattered lines) based on certain rules. Under a framework, mobile nodes may perhaps be allocated a dissimilar position or gathering, such as crowd together Chief-head, cluster member or cluster gateway [12].

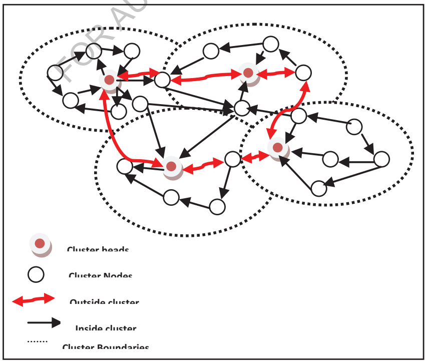


Figure.1: Cluster composition design

An assemblage chief habitually provides as a neighbourhood controller for its grouping of huddle, the stage intra-group huddle televise assortment, forwarding the in rank and so on. A huddle entryway in non-cluster cranium mobile knot with inter-cluster paths, so it can contacts candidate clusters and promote in sequence flanked by clusters. A group cluster associate is frequently defined as a normal node, which is a non-cluster head knot devoid into any inter-cluster acquaintances.

Intention of this job will widen the cluster based privacy preserving direction-finding code of behaviour [1] in MANET framework is actual fact partitioning in and out huddle memo spread in safe and sound behaviour. To minimizing a load balancing of low-maintenance clustering schemes intend at provide secure cluster framework flow for huddle base steering protocol in midst of slight bunch preservation outlay. By precautionary re arrangement of clustering positions or low-minimizing precise be command of packets for clustering, the crowd together configuration is able to be sealed well without extreme utilization of classification property for crowd together preservation.

Respite of the content organized as follows: Literature reassess detailed into Section 3 and 4, Load Balancing Clustering Process is explained. Section 5 Evaluation of presentation is carried out and section 6 referred as conclusion.

3. Literature Review

(*R. Jayaprakash*, *B. Radha*, 2018) proposed a solitude preserving network of collection, bunch ch reliable for message with connections during a huddle which uses added sequence (energy) pre-eminence of assessment to huddle members a gather assemblage. As a packet (information of message) spread in and out of huddle as a consequence, it becomes an extremely testing job to preserve steadiness in network. Aimed to present a "cluster based privacy preserving routing protocol [1] selection algorithm in in and out cluster" using NS (Network Simulator) 2.34 Framework. The direction-finding etiquette assortment based Cluster head medley prototype operates completely based on starting place routing, required-demand progression, it has been selected as course-plotting code of behaviour be worked and knowledgeable for ad hoc set of connections capitulation differentiated into a basis sought announcement exchange intermediate mobile points in a convenient network [1].

(*Mahesh K Marina* and *Samir R Das*, 2002) developed [2] based on demand of multi-path detachment vector protocol" for itinerant ad hoc networks. Predominantly, they proposed many path expansions to a correct definition distinct path routing protocol recognized as on-demand detachment vector (AODV). The consequential protocol is described to as ad hoc on-demand multi-path distance vector (AOMDV). The code of behaviour calculates compound loop-free and path-un join links. Freedom of loop was assured by use a perception of "advertised hop method of count". Hook up dis-joint of numerous links is attained by using exacting assets of broadcasting. Recital assessment of AOMDV with AODV using network simulator demonstrates the AOMDV is proficient to attain an incredible improvement in the laterally delay-often additional to an issue of two, and is what's more capable of decrease routing disbursement by 20%.

(*Oussama Souihli, Mounir Frikha*, and Mahmoud *Ben Hamouda*, 2009) [1], Discussed the Mobile ad hoc networks (MANET) be framework of less networks, with dynamism fashioned by an autonomous arrangement of nodes that are associated using without wire links. Since routing is executed by points with incomplete possessions, load [3] should be competently scattered throughout the arrangement. Or else, loaded nodes could create up a restricted access that lesser the network presentations through jamming along with superior wait. Unfortunately, weight equalling is a significant scarceness in diminutive path steering protocols, as mobile at the middle of the network are greatly heavily-loaded over than the others. The authors proposed load-balancing methods that thrust the reassign ancillary from the middle of the n/w. essentially; they provided steering metrics that take into plot nodes grade of centralized [3], for both down to business and involuntary direction-finding protocols. The results showed that the proposed mechanisms progress the weight allotment and extensively improve the association improvements in surroundings of normal impediment and dependability.

(*Y. Ganjali* and *A. Keshavarzian*, 2004) illustrated a multi-path [4] direction-finding has been considered methodically in the circumstance of on edge networks. It has been open to the elements that using several links to direction information's concerning several sources to designation couple of mobile nodes balances the weight supplementary consistently during traversal. The numerous faiths are that the equivalent is perfect for ad hoc n/w, i.e., multi-path routing stability the load considerably improved than single-path routing. They showed that this is not essentially the case. They introduced latest model for assessing the weight balance below different-path routing, when travelling paths are selected are the primary K- shortest paths. With this representation, they showed that except we use an extremely huge number of links the load allocation is approximately the similar as single shortest path routing. This is in different to the earlier obtainable results which believe that multi-path routing distributes the load consistently.

(*Y.J. Lee* and *G.F. Riley*, 2005) offered extremely successful technique to attain load steadiness and overloading improvement. The novel method is annoyed by the examination that ad-hoc on-demand course-plotting protocols screen direct demand (*R-REQ*) [5] packets to obtain paths, as well as cleanly mobile nodes with the intention of act in response to those packets have a possible to supply as between promoting mobile nodes. Stipulation a node disregards R-REQ packets within a particular period; it can entirely be barred from the further exchanges that might have happened for that time or else. Thus, a mobile node can choose not to provide a traffic flood by reducing the *R-REQ* for that flood. In the novel method, R-REQ packets are promoted selectively according to the load condition of every mobile node so that overloaded nodes can be barred from the demanded links. Every mobile node starts to permit added traffic flows over at any time its overloaded status is softened. The novel method operates boundary line residence and work to manage R-REQ packets adaptive manner [5]. The superior methods of protocols with this method are equal to the support protocols.

(*Mahdi Abdulkader* and *Raghav Yadav*, 2016) focused on assessment and inspection of competent weight equalling policy of behaviour intend for MANET [6]. Bungling load corresponding method results in growing routing transparency, reduced carton transferable value, and bonus as Quality of Service overhaul (QoS) constraints. In text, there are sums of dissimilar methods of findings for recovering the presentation of direction-finding protocols by competent load balancing amongst mobile nodes statement. Though, the greater part of the techniques suffered from different restrictions. They proposed a method for enhanced the Quality of services act of load balancing precede as well as growing the system time period.

(*M. Hasanpour, et.al.,* 2017) presented a narrative move towards in objecting weight debating in ad hoc networks employing the quantum [7] diversion assumption. The method profits from the immediate and message-less ability of knotted fundamentals to coordinate the load comparison policies in ad hoc networks. The quantum credence evaluation (QLB) technique projected by job is development on stratum of link State steering as the common line steering protocol; its staging is examined beside the baseline OLSR, and substantial growth is accounted concerning numerous of major quality metrics such as intermission and dwindling of error-jitter. In addition, it is exposed that QLB modus operandi ropes an unyielding steadiness increase in stipulations of performance which positions a substantiation opinion in favour of the weight paired mode of described hypothesis.

(Jayaprakash R, Radha B, 2017), acknowledged that CBPR in portable network distance of inside cluster and as well as outside cluster gives new path for creating new findings and techniques in large group of networks[13].

(*Benjamin Sliwa*, *Robert Falkenberg*, *Christian Wietfeld*, 2017) discussed a resourceful direction-finding is single of the solution [8] confronts pro subsequently creation transport system in arrange to offer rapid and dependable message in an elegant city circumstance. A diversity of map-reading protocols has wished-for shaping best paths in extremely active topology. Conversely, it is quandary of individual things of networks that superior quality links are used resultant in purpose of jamming and link excellence in dreadful state of affairs. The authors adopted ideas from different path routing along with proposed an easy de-central scheme for node based routing, idea moves flaccid weight balancing elite of involving auxiliary announcement stab. It can simply be well-designed to easily reached distance-findings protocols to accomplish load debating deficient varying the routing process itself. In inclusive facsimile learns, they applied the load estimation method to manifold instance protocols and assessed its belongings on the network concert. These consequences showed all measured protocols attain noticeably elevated dependability in addition to better-quality proportion of container content deliverance (PDR) principles by unfolding the future weight estimation process.

4. Load Equilibrium and Cluster Process

Load equilibrium balance in huddle process judge that there is premium comes to nodes (*mobile nodes*) that cluster can hold, particularly in chief based MANET. Too-Large huddle puts too cumbersome weights on head for passing that makes results into jamming of system (throughput). Small crowd together might take benefit to craft a mammoth amount of huddle and consequently boost/increase the total time-span of paths that results in generous laterally setback. Load-balancing process in huddle locates higher to subordinate confines add to points that a huddle be capable of squashed with. When [4] a determine value is exceeded we want to make a new re huddle process for the originality with the points. The diagram indicates the Load evaluation group Based isolation Routing flow.

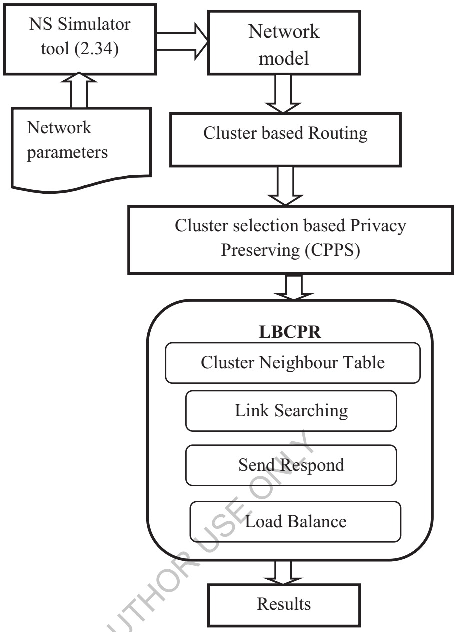


Figure.2 Load Balancing Cluster Based Privacy Routing (LBCPR) Flow

Neighbour node identified for assembly arrangement as the result in cluster head and its corresponding members are selected. Main theme to identify the clusters which huddle is nearby to transfer of packets. With the help of neighbour counter, we can identify the cluster and its member within the shear zone or not. We can also identify the path which is more comfortable to transfer the packets from one node to the other node.

By facilitate of Link search notation, useful to find the link between clusters that for a connecting purpose. If node ready to link with other clusters, accept request and respond to based on load balance carry. Load be balanced to the every node then only we can find the optimal solutions otherwise it may result in gaming, delay in PD ratio and etc.

4.1 Arrangement of Network representation

In set of connections arrangement process is evaluated in graph diagram configuration was before now presented by (*R. Jayaprakash*, *B. Radha*, 2018) [1].

In this model, the system will described a network with the following assumptions:

1. The network model is defined where every cluster is controlled by the "cluster chief" called manager node.

2. The association includes the inside cluster and outside cluster communication.
3. The data renovation is performed through cluster chief.
4. Positions of all nodes and orientations are dynamic.
5. If the controller nodes are present, it will control a group of nodes
6. An arrangement can have one or more locations depending on the network region and compactness.

4.2 Cluster based Routing model

This cluster based routing method reduces the routing in sequence received and promoting information retained by every node from O(N) for a non-hierarchical direct assembly to O(mnCmax) for an mn-level hierarchical control relationship of nested clusters, where Cmax is the upper limit number, over all i, of particular level based-i cluster proscribed within a increase level(i+1) method of cluster. Huge values of mn and random sources and targets, this cluster-hierarchical routing method may give way paths whose costs are better than those of the right minimum-cost paths. However, in scrutinize clusters are shaped with only a small quantity of levels and the cost variation is often small.

This routing method, “Mobile nodes generation”, “Circulation”, and use cluster-hierarchical routing information as follows. Every node within level-1 cluster broadcasts, to further mobile nodes inside the cluster, its link state order stated as link cost to its contiguous nodes. The intact nodes then assemble minimum-cost paths using lasting pathway algorithm to all other nodes inside that cluster. Every gate way node on the edge of a cluster uses inside-cluster link state information to evaluate every other gate for the cluster. A gate then constructs link state in sequence in interspaced-vector and link-state cluster-hierarchical routing schemes can be applied as hybrid schemes for routing in outsized premeditated message networks. In this scheme, every node eventually uses interspaced-vector routing to launch the next hop on the minimum-cost route to every objective, but for objective outside of its cluster the interspaced-vector routing in sequence is in component resultant from link-state in sequence between inside and outside clusters.

4.3 Cluster Based Privacy preserving selection (CPPS)

A CPPS node chooses itself as cluster-head if it does not accept control messages from several cluster-head or if it accepts control message hype two special separation identifiers. The CPPS algorithm performs the following methods to boundary the number of mobile nodes concomitantly attempting to become cluster-heads:

1. All nodes that notices one of the constraints for becoming cluster-head ruins a small random time interval and tests over the constraints. If the constraint perseveres subsequent the tentative period, the mobile node assumes the location of cluster-head.

2. Each one new cluster-head instantly concerns control messages in rapid sequence declaring its status.

Clustering ("Huddle") makes feasible en route on behalf of declare basic stipulations - cataloguing recital, next to same time as throughput and impediment, in occurrence both diminutive and bulky itinerant terminals.

4.4 Load Balancing Cluster Based Privacy Routing (LBCPR)

LBCPR direction-finding formations headed for shore up stack pondering enlargement,

- C N Table
- TH topology (Two-Hop)

CNT accumulates in sequence about nearest cluster, whether it comes out as bi-directionally or one direction method of connected.

- In Bi-direction method link between two mobile nodes there exists less amount of one way path between two nodes.
- Uni-directionally modelled method is about only one path is available for those nodes. i.e. form sender and the collector

In figure 3, X, Y and X, Z are two-way directionally linked, clusters Z, W is one way directionally linked.

In LBCPR works based on innovative metric called weight (Load), thus instates to calculated load of mobile node (mn) is decisive in current system, its assessment will indicate the enumerate of present load. The Load tells attribute in every one privacy route R_REP data packets to allow the starting place in selecting a link that assures superior load steadiness based on two scheduled criterions [1]:

1. Minimum value - load amongst all promising nodes as subsequently hop.
2. Comparatively smaller hop reckoning than the finest link.

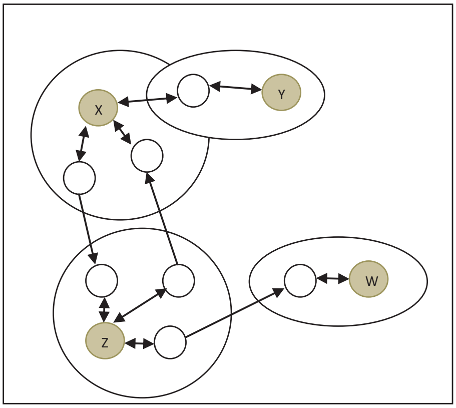


Figure.3 connecting among clusters

The number of acquaintances flanked by nodes can maintain, in concentrate focal point to a fitting starting path – objective node. Link can be understand by the amount of seclusion R_REP packets that path back to sources (starting point). Intuitionally, LBCPR can argue that if a R_REP is route support a "lofty likelihood that the matching nodule will donate as a middle hop for message transfer". So, the ending is, greater the R_REPs in retreat back through node, healthier load furthermore well again the odds for to centre nodes of the system / else, if scene conjecture is not headed for be forced, then can still supervision scheduled to equitable load weight part of node is be alleviated.

Proposed LBCPR picks up acquaintances will reassurance smaller quantity loads. Less loads, we average point at forefront of not here on or after centre. Civilizing centre nodes from weight inequality moreover serving in permanence of coupled model.

Algorithm for Link Searching

```
Intialize $link \leftarrow 0$; routing table $rt \leftarrow 0$; $load \leftarrow 0$; distance $dsst$;
Process
if $link = rt \rightarrow rtsearch\ (dsst) \neq 0$ then
while link $\neq 0$ do
//To obtains verification with minimum weight between next accounts.
if $link = load \rightarrow load \leq rtminload$ then
//rtminload will have the minimum load among all next-hops for that destination
Move_forward (link, message);
break;
end if
link = link → next
end while
end if
```

The algorithm for send respond is stated below as building the new RREP data packet. Notice packets contain in sequence to load field this load be abridgment of load with intention to provide path undergoes and the nodes load as the intermediary node. Verification carried to find minimum load between hop records in addition to consolidate minimum load of next hop just before target. On behalf of clarity purpose pertaining to load only shown / noted other considerations are omitted.

Algorithm for Send Respond

```
if link = rt → rtsearch(dst) $\neq 0$ then
 while link $\neq 0$ do
   if link → load $\leq$ rtminload then
```

```
      rpdst = link → nexthop
      rphopcount = link → hopcount
      rpload = link → load + load
      rpexpire = link → expire + CURRENTTIME
     break;
   end if
  link = link → next
end while forward(rpdst,p);
end if
```

5. Performance Evaluation

The proposed scheme consists of 50+1 knob in huddle Based load solitude Routing (LBCPR) in mobile set-up, with nodes arbitrarily fitted for exploitation in span of 300x300 m. The imitation values of parameters is given below,

Table 1. Simulation Parameter

PARAMETERS	SYMBOL	VALUE
Nodes of the mobile	MN	Stepladder of 10 (5 to 50)
Simulation Area	Row × Column	300 × 300
Range of transmission	TR	5 to 50 in ladder of 10 times
Distributed Weights	D_{w1}, D_{w2}, D_{w3}, …, D_{wn}	(0.1, 0.04, 0.05, 0.2, 0.5)
Node Energy (In terms of Power)	E_{node}	100Joules
Boosting Energy (Enhancement need)	E_{boost}	100J/bit/m^2

The Energy container deliverance proportion can be calculated based on the number of packets generates and passed by source initiative node and the packets received by the designated point in products. This projected scheme works in terms of PDR by distributed weight cluster manner.

$$EPDR = \left(\frac{Amount\ of\ Sending\ \ messages}{Amountof\ Receive\ messages}\right) \times 100 \qquad (1)$$

EPDR is Energy Packet Delivery Ratio

Packet delivery ratio can be predicted by the terms of amount of packet send and the amount of packet that received in particular time.

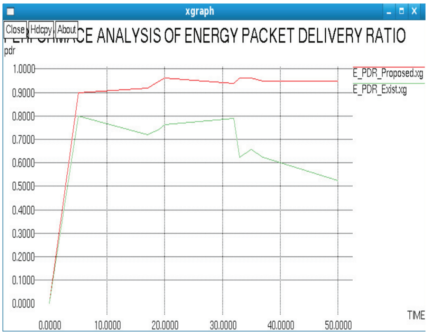


Figure. 4: Performance analysis of Energy packet delivery ratio

The association to get-up-and-go performance of the classification indicates old and new proposal way next to differentiate with red line as ground-breaking finding and emerald as old finding value of the conventional techniques of cache method. Graph: *Y* axis formulates the performance values and the *X* axis formulates the time duration value in system experimentations tool.

$$EX = \frac{\textit{Number of message requests}}{\textit{Total Time duraiton}} \qquad \textbf{(2)}$$

EX is performance analysis of throughput ratio,
Throughput ratio can be resolute by the integer of demand message packets within the given amount of time scheduling.

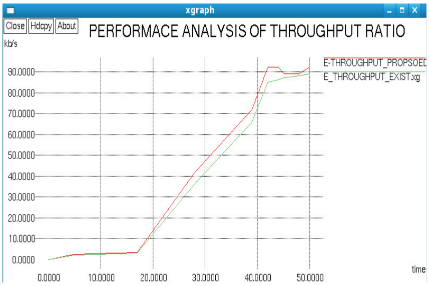


Figure. 5: Performance analysis of Throughput ratio

6. Conclusion

Work evaluated and analyzed the [1] Load Balancing Cluster Based Privacy Routing (LBCPR) algorithm for mobile ad hoc networks on the strength of connection and head selection formation. The LBCPR load disparity in network and preconception or nepotism during finding of common positioned nodes for transportation of datagram's [1]. Meanwhile, projected system establishes a modified cluster based routing and Cluster Based Privacy Preserving Selection (CPPS) protocol called Load Balance system the complete instrument engaged in balancing load.

References

[1] R. Jayaprakash and B. Radha, "CBPPRS: Cluster Based Privacy Preserving Routing Selection in Wireless Networks", IJET, UAE , vol 7 Iss (3.12) pg:439-443, 2018.

[2] Mahesh. K Marina and Samir R Das. "Ad hoc on-demand multipath distance vector routing", ACM SIGMOBILE Mobile Computing and Communications Review, vol 6, iss:3: pp: 92-93, 2002.

[3] Oussama Souihli, Mounir Frikha, and Mahmoud Ben Hamouda "Load-balancing in manet shortest-path routing protocols", Ad Hoc Network, vol 7(2) : pp 431-442, March 2009.

[4] Y. Ganjali and A. Keshavarzian, "Load balancing in ad hoc networks: single vs. multi-path routing". Conference of the IEEE Societies, volume 2, pages 1120-1125 vol.2, 2004.

[5] Y.J. Lee and G.F. Riley. "A workload-based adaptive load-balancing technique for mobile ad hoc networks", Wireless Communications and Networking Conference, IEEE, volume 4, pages 2002-2007 Vol. 4, 2005.

[6] Mahdi Abdulkader and Raghav Yadav , "Efficient Load Balancing Routing Technique for Mobile Ad Hoc Networks", International Journal of Advanced Computer Science and Applications, IJACSA , Vol. 7, No. 5, pp 249-254, 2016.

[7] M. Hasanpour, S. ShariatP. BarnaghiS. A. HoseinitabatabaeiS. Vahid R. Tafazolli, "Quantum load balancing in ad hoc networks", June 2017

[8] Benjamin Sliwa, Robert Falkenberg, Christian Wietfeld, "A Simple Scheme for Distributed Passive Load Balancing in Mobile Ad-hoc Networks" , Vehicular Technology Conference (VTC Spring), 2017.

[9] Bednarczyk. W, P. Gajewskil, "An enhanced algorithm for MANET clustering based on weighted parameters", Universal J. Commun. Netw. Vol 1(3), pp:88–94, 2013.

[10] Chatterjee M, SK Das, D Turgut. (2002). "WCA: a weighted clustering algorithm for mobile ad hoc networks"vol 5, pp:193–206 KA Publishers, Netherlands, 2002.

[11] Chiang C, H. K Wu, W Liu, & M Gerla "Routing in clustered multihop, mobile wireless networks with fading channel. Proceedings on IEEE SICON'97. pp. 197–211, 1997.

[12] Ephremides, Jeffery Wieselthier, Dennis Baker. “A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling” Proceedings of the IEEE Vol 75,No. 1, pp. 56-72.1987.

[13] Jayaprakash. R, Radha. B, ” Review on Routing Protocols and Privacy Preserving Cluster Based Protocols in Wireless Networks”, IJARSE, Vol 6, No.12, 2017.

[14] JY. Yu, PHJ. Chong, “A survey of clustering schemes for mobile networks”. IEEE Communication Surv. Tutorials, vol7(1), pp:32–48 2005.

[15] C.H. Liu, B Rong, S. Cui, “Optimal discrete power control in poisson clustered ad hoc networks”. IEEE Transaction Wirelesss Communication, Vol 14(1), pp: 138–151, 2015.

Chapter - 05

DLBPS: DYNAMIC LOAD BALANCING PRIVACY PATH SELECTION ROUTING IN WIRELESS NETWORKS

Abstract. The Adhoc Network (MANET) is a set of nodes inside a particular group which communicates one another inside the network. These are generally packet nodes that travel and subjected for variation in the routing based on the requirement of the mobility. A proper routing technique is essential for the transmission of data packet from the source to the destination. A cluster based routing protocol is accessed on its capability to distribute transfer over the network mobile nodes and a superior routing protocol realizes this without establishing unacceptable delay. This paper presents novel Dynamic Load Balancing Privacy Path Selection (DLBPS) algorithm for mobile ad hoc networks to address the issue of the packets’ strength when transmitted and also on the security aspect by addressing attack prevention. The experiment is carried out as a simulation in NS2 framework. The DLBPS method performs gateway mobility load balancing in the network order to achieve higher aggregated throughput among data transfer. Meanwhile, the proposed algorithm establishes detection, privacy collector privacy manager and privacy propagator to complete the privacy path selection. The experimental result proves that the proposed mechanism outperforms the existing HsecGR and Trust-ECC methods.

Keywords: Cluster, Load Balancing, Gateway, Privacy Preserving, Path Selection.

1. Introduction

A Mobile Ad Hoc Network (MANET) is a kind of Ad Hoc Network that consists of many nodes that are mobile and wireless in nature forming a temporary network in the absence of the support from stable “network infrastructure”. In MANETs, all nodes are capable to move and still connected using multi-hop communication. The foremost goal of this network is provisioning of efficient communication by incorporating routing functionality into mobile network nodes. A MANET network is decentralized networked system where the nodes themselves are responsible for all activities within the network such as topology discovery and packets or message delivery.

The MANET can be logically depicted in the form of clusters through assembling together group of nodes that can be managed by cluster heads. Within a particular cluster, the cluster head (CH) is interconnected to all the nodes in its cluster [3], (*Chatterjee M, SK Das, D Turgut*, **2002**). Clustering is vital technique in a MANET often utilized to structure its hierarchy and organization. The use of clusters assists to simplify the complexity in how information about cluster nodes are managed as well as approaches to resolving or reducing network blocking.

Cluster based routing is one of the routing methods with regard to MANETs (E*phremides, Jeffery Wieselthier, Dennis Baker*, **1987**) [5] in which several clusters of mobile nodes tend to be shaped using each cluster featuring its own cluster head that accounts for routing between clusters. "Clustering of nodes saves energy along with transmission bandwidth in ad-hoc networks".

2. Cluster Network Model

In the adhoc network, the packets are sent from a source to destination using the multi-hop approach by selecting a suitable nodes in the middle Data are transmitted across a peer to peer network in the absence of a centralized server in the available protocols . These are organized dynamically by self as in case of an adhoc topology.

Clustering (*Bednarczyk W, P Gajewskil*, **2013**), [4] is a methodology where relatively large network is segmented into smaller groups having some characters or behavior in a similar fashion. This is done based on some protocols in order to make the difference visible in-between the available nodes in other sub networks. The nodes which are not related to each other are combined to arrive at a structure. All nodes are assigned predefine functions and constraints namely cluster head, the gateway and nodes of the member of cluster. This the area which is segmented is called a cluster which bears a head and acts as a co-ordinator and are selected by every cluster.

Cluster head (CH) are similar to other nodes but performs the functionality as a supervisor and are responsible for functions such as cluster management, updation of routing table and are responsible to identify new routes. All the other nodes are members inside a cluster and the node through which the inter communication occurs are called as gateway nodes. The Cluster head is responsible for the data transmission among the nodes inside a cluster and outer communications if any are done through the CH through the gateway nodes.

The clustering is done in a way that all the nodes inside a cluster are subjected to transmit a HAI or Hello message along with their IP address. The CH in further appends the IP address of the nodes that are members to their self messages that are controlled. The connection is considered as broken if the member node fails to get three control messages in the process of selection of clusters. In case of broken communication, The corresponding node go in search of a new CH. To confirm the new CH, The hello message is transmitted along with its IP address.

The objective of the research is to propose a protocol for routing which is based on the cluster technology and which is privacy preserving in a MANET. Environment, The main aim is to effectively partition the inside and outside broadcasting of cluster message in a secured fashion. . To minimizing a load balancing of low-maintenance clustering schemes intend at provide secure cluster framework flow for cluster based routing protocols with slight cluster preservation cost. By preventive re-clustering positions or minimizing precise control packets for clustering, the cluster configuration can be preserved well without extreme utilization of network resources for cluster preservation.

The remaining of the paper is segmented and presented as follows: Literature Review is detailed in Section III, In Section IV we have discussed about, Dynamic Load Balancing Privacy Path Selection (DLBPS). Section V, VI about the Performance Evaluation and Conclusion respectively.

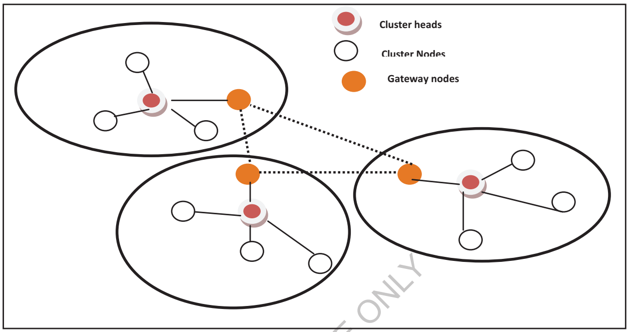


Fig. 1: Cluster network model

3. Literature Review

(*R. Jayaprakash*, *B. Radha*, **2018**) [1],[2] came up with the networking group in which the privacy is preserved, Here the CH is responsible for the inter communications inside a cluster with the aid of a battery in addition which is dominant in evaluating the members of the cluster. As the information packets are subjected to go in and out of the network, The overhead in testing the stability of the network becomes crucial. A routing protocol based on the clustering technology is proposed to achieve privacy preservation. The experiment is simulated using the NS2 tool . The complete process was based on the routing that happens in the source and on demand process. The peoposed protocol is based on the CH selection and the same is applied in adhoc framework by a variation by implementing a communication exchange on demand between the nodes that are mobile in a adhoc network.

(*Gupta, A.K., Sadawarti, H., Verma, A.K*, **2011**), [6] pu t forth the problem when routing is considered and the research challenges in the MANET environment and got a large number of responses from the researchers round the globe. In order to address the problem associated with routing , various protocols were proposed and still researchers are working for man more such protocols to be proposed. To identify the best protocol is a tedious task as the behavior and performance of each protocol varies in different scenarios as when size and topology of the network are considered. The detailed surveys of the existing protocols are elaborated with its functions and characters. A comparative study was also made on the available methods that are very much used for arriving at an routing decision.

(*Kaur, H., Singh, H., Sharma, A*, **2016**), [7] explained the concept of MANET which are tented to have organized in a self mannered networks through which there is no need of connections to be established for the transmission of information. These suffer from different factors interms of scalability, topology and higher mobility. These are also subjected to damage owing to its large mobile nature. Routing on the basis of the topology are subjected to fail because of the dynamic change in the topology itself. A new concept of routing based on the geography of the nodes was introduced. These proved to be more stable and efficient even in the case of dynamic change in the location of the nodes. Two methods namely the hybrid routing and geographic routing are studied in this paper

(*Sarika, S., Pravin, A., Vijayakumar, A., Selvamani, K.*, **2016**) In wired networks, [8] thre are a large number of barriers when communication occurs. These pave way for the intruders to get pass the firewalls . Hence these have to made to got through secured gateways for safe transmission of data. Unlike the wired networks, The wireless sensored networks are considered to be less safe as the nodes follow a dynamic topology and also the power consumed will be more . The mobility is the key factor to be taken for account as it paves the way for attackers leading to collapsing the complete network. The problems associated with the wireless mobilenetworks are discussed in detail.

(*Boulaiche, M., Bouallouche-Medjkoune, L*, **2017**), [9] proposed a new technique which takes into account of the geographic locations and came up with a routing concept based on the location of the nodes under communications from source to destination. These also reduce the overhead of routing control and guarantees accurate delivery of the message without time delay over such networks. The basic problem with this approach being that all the nodes are considered as trusted which paves the way for malicious content which in turn disrupts the forwarding of the packet. A proposal was given for the new approach for the security against attacks possible. The nodes that lies in between are tested for its authenticity and integrity and sends back the acknowledgement upon verification. This prevents the packet being dropped in middle due to attacks. Symmetric cryptography is used as an encryption standard . They proved to be efficient even if there are compromised packets in the network.

(*Kaur, M., Kaur, S*, **2016**), [10] discussed routing protocols methods are employed to send as well as obtain information from origin to vacation spot correctly. Clustering structured routing protocols methods are the methods through which course plotting will certainly done by means of grouping. Clustering is often a practice where a big network is divided right small groups as well as communities. The leading purpose of clustering is usually to boost routing protocols in the network stratum through reducing the size of the particular routing protocols platforms as well as lessens improve over head through updating the particular routing protocols platforms soon after topological alterations take place. This kind of report is evaluate as well as apply the particular functionality associated with current cluster structured routing protocols method that the election associated with cluster go is dependent on the particular minimum Ids associated with node in cluster. The authors evaluated the particular functionality associated with CBRP method as well as present each of our outcomes.

(*Rajasekar, S., Subramani, A.,* **2016**), [11] briefed that a MANET has a great number of nodes that are subjected to move in a dynamical manner . In such networks, The devices used for computation will require a large and costly infrastructure. In these networks, The nodes are subjected to move dynamically from one place to other and try to get synchronized with other nodes that are nearer. Te topology can also change due to the mobility aspect. The main limitation of the MANET is the energy that will be available for each node for successful transmission and the life time of a node. Hence the energy efficiency is a vital factor and was discussed elaborately.

4. Dynamic Load Balancing Privacy Path Selection

It is a vital process that aims to control the traffic in a complete network and also assures of distributing the traffic evenly over the network. The load will not be evenly distributed if there are user demands that are un even and are more common in case of a MANET. The nodes present inside a network gets more congestion and naturally vulnerable as a consequence owing to the fact of their location and the role assigned to them. The congestion will normally be more at the centre rather in the end due to the fact that major of the nodes travels through the centre part else would be put in a position to have contented with the relatively large number of neighboring nodes in the medium. The gateway nodes are subjected to more congestion since the traversal have to be done through the intermediate traffic domain. The congestion has to be avoided in such cases to maintain the connectivity in the network and the services they provide. The figure 2 depicts the Dynamic Load Balancing Privacy Path Selection (DLBPPS) approach.

4.1 Network and Mobility Model

In process of network formation [1], [2] is ranked by forming graph ans was already presented in the previous work (*R. Jayaprakash*, *B. Radha*, **2018**). In the Mobility model, V_{max} and T_{pause} denotes the two important key metrics that depicts the node's behavior. If the V_{max} is minimum and the pause time T_{pause} is long, there exists a strong topology which will be more stable. Contrarily if the speed of the node is more, (i.e.,V_{max} is more) and time of pause is T_{pause} is lessm There will be high dynamicity among the nodes.. By changing the values of these metrics, different scenarios for mobility can be achieved for variety of n ode's speed. The metric of mobility is to calculate in a quantified notation of the node's notation speed. This relative measure of speed between the node i and j at a given time t is

$$Speed(i,j,t) = \left| V_i(t) - \frac{V_j(t)}{M} \right| \quad (1)$$

The metric of the mobility is then calculated with reference to the speed in a relative manner which is taken as a mean of all the speeds in all the pairs of nodes in the entire time. The function is denoted with a formal notation as

$$M = \frac{1}{|i,j|} \sum_{i=1}^{N} \sum_{j=i+1}^{N} \frac{1}{T} \int_{0}^{T} Speed(i,j,t)dt \quad (2)$$

where $|i, j|$ is the count of pairs of node that are distinct n is the overall count of the node in entire field of simulation. (i.e., the complete ad hoc network) and T is the time of Simulation.

4.2 Gateway Mobility Load Balancing

This is a task of even distribution of inter domain traffic in an orderly manner and also efficiently in between the gateways and the primary objective being to increase the throughput as depicted in Figure 1. The primary pre condition is that it should have more than one gateways that are placed in the network which ensures the connection to the gateways present outside the network for transmission. This can also be the internet. All the inter-domain traffic are subjected to go through the nodes that are the gateways, They become more congested and hence many gateways needs to be deployed in the network which enables the complete capacity of the network increased and the probability of congestion decreases.

The redundancy is also reduced which paves the way for increases robustness. If any of the gateway experience a failure, The others that are in standby will take care of the network. The policy of fairness is also achieves as with single gateway , different nodes enjoys different capacities that are based on the gateway's proximity. The mean distance to reach the gateway will be same in case if many gateways are deployed. Even though, this technique proves to be more efficient than others, it also suffers some drawbacks. The traditional methods lacks a concrete method to overcome these issues. When a short path is arrived, There are more possibilities that a gateway will be overloaded leading to collapse in the entire network. Hence appropriate load balancing techniques are to be deployed for removing the potential risk involved and to ensure that there are no degrade in the aspect of performance. Cluster Based Privacy Preserving Routing Selection (CBPPRS) [1] is already elaborated in the previous work (*R. Jayaprakash*, *B. Radha*, **2018**) . Here a DEFINED-VALUE concept is used between he CHs and the nodes such that all the nodes in the given time of a network are within h hops of a CH.

4.3 LBCPR: Load Balancing Cluster Based Privacy Routing

The LBCPR was already we presented (*R. Jayaprakash*, *B. Radha*, **2018**) [1], [2] load imbalance in the network and the partiality or favoritisms in picking up centrally located nodes for data transfer. The proposed a novel cluster based routing metric, load and a minimization principle to make a decision a path that occupies mobile nodes with fewer load weight on them In LBCPR performs new metric called *load* will tells us the estimated load a mobile node (*mn*) is focused to in a network, its value will specify the quantify of current load. In this model, link searching and send respond algorithms performs cluster load field accurately.

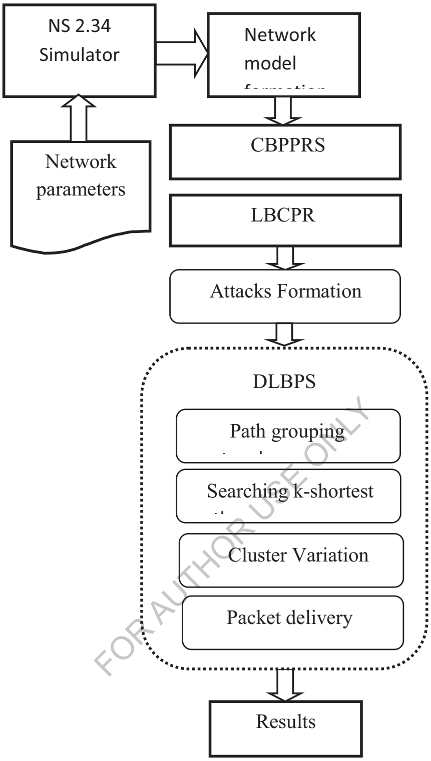
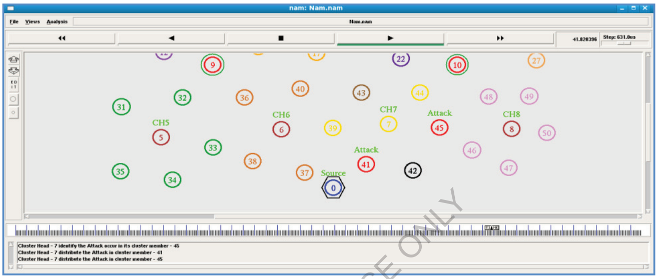


Fig. 2: Dynamic Load Balancing Privacy Path Selection Flow

4.4 Dynamic Load Balancing Privacy Path Selection (DLBPS)

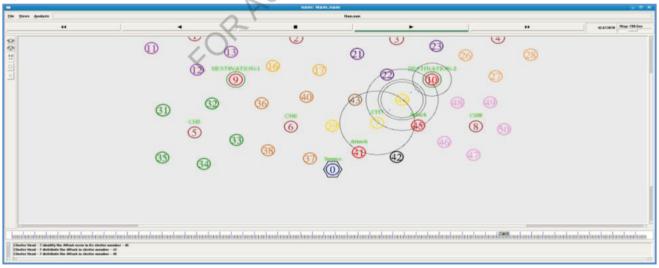
The DLBPS searching is achieved by k-path measure in the MANET and this can be either in one direction or two direction. Hence the host must be knowing its neighbor and the related information. The data packets are transmitted on a regular interval of time by sensing the neighbors. These are transmitted only a hop away and are not pushed further. When the host 1 gets the Hello message from Host II , The status of the second host is set to be asymmetric in the routing table.

DLBPS algorithm also helps in predicting the attacks that are distributed in an MANET. The scheme of investing the scheme's path of a protocol will examine all the nodes in the available network and when any unusual behavior is found, the invocation of a distributed algorithm is done to confirm that the node is out of any malicious content. This method works along with other security metrics which are available in every node inside a network. The computations are given in terms of .: (i) Detection, (ii) Privacy Collector, (iii) Privacy Manager and (iv) Privacy Propagator.



```
Cluster Head - 7 identify the Attack occur in its cluster member - 45
Cluster Head - 7 distribute the Attack in cluster member - 41
Cluster Head - 7 distribute the Attack in cluster member - 45
```

Fig. 3: Attacks Formation



```
Cluster Head - 7 identify the Attack occur in its cluster member - 45
Cluster Head - 7 distribute the Attack in cluster member - 41
Cluster Head - 7 distribute the Attack in cluster member - 45
```

Fig. 4: DLBPS Result

Algorithm 1: ***Dynamic Load Balancing Privacy Path Selection (DLBPS)***

Intialize *CH*← 0; *LBCPR*← 0; *DLBPS*← 0;

Process

```
Step 1: The node has to travel from source to destination through a protocol which starts the identification of the route.. During the identification process, source node transmits RREQ packets through the nodes which are available nearer.

Step 2: Searching neighbor cluster list present source        to destination.

Step 3: Check gateway mobility balancing (gmb)

Step 4: if $gmb \neq CH$ then
        CH = $CH + 1$
        end if

Step 5: if gmb_count> nodecount_thresh then
        //Target and all previous nodes are declared.
           forward (attack link);
            break;
        end if
Step 6: select privacy cluster path for packet delivery
```

5. Performance Evaluation

The proposed system considers 50 to 200 nodes *Dynamic Load Balancing Privacy Path Selection (DLBPS)* in mobile adhoc network, with nodes and are implemented on a random basis in a area of 1000 m × 1000 m. . The parameters considered for simulation are as mentioned below. Packet delivery ratio (PDR) is described as the fraction between the number of packets sent and received in destination. The proposed method ensures more PDR ratio when compared with existing HsecGR [12] (*Boulaiche, M., Bouallouche-Medjkoune, L*, **2017**) and Trust-ECC (*S. Syed Jamaesha and S. Bhavanim*, **2018**) methods [13].

Table 1: Simulation Parameters

PARAMETERS	**SYMBOL & VALUE**
Mobile Nodes	MN & 5-200 in steps of 10
Simulation Area	Row × Column & 1000 × 1000
Transmission Range	TR & 5-200 in steps of 10
Distributed Weights	$D_{w1}, D_{w2}, D_{w3}, \ldots, D_{wn}$ & (0.1, 0.04, 0.05, 0.2, 0.5)

Node Energy	E_{node} & 100Joules
Boosting Energy	E_{boost} & 100J/bit/m^2

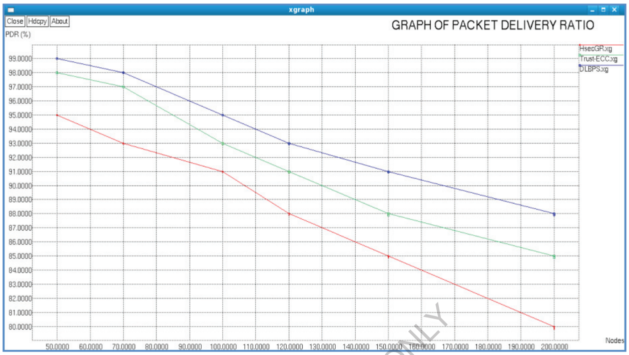


Fig. 6: Graph of packet delivery ratio

The throughput is comparison is shown in figure 7 where the blue line indicates the performance of the proposed algorithm and the red and green line of the performances of other existing methods. [13] . The performance is measured by taking the average throughput in Y axis and number of nodes in X axis

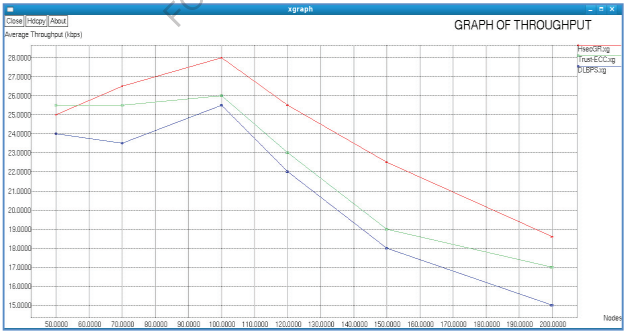


Fig. 7: Graph of Average Throughput

In fig. 8 depicts the average performance delay and it is obvious that the proposed method out performs the other existing proposals[12][13]. The Average delay performance is taken as the product of time taken to get and deliver a packet. describes the Average delay of performance result. It is the product of time taken to obtain packets delivers to number of mobile nodes in network.

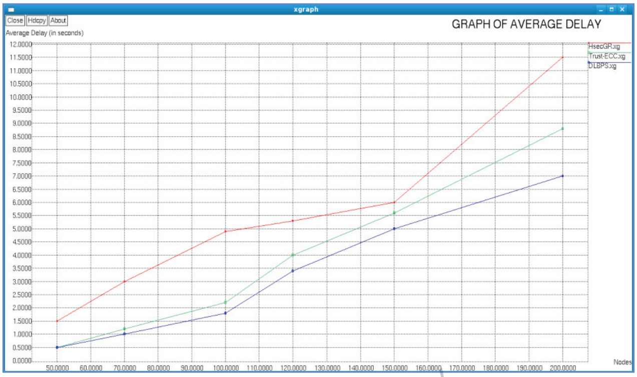


Fig. 8: Graph of Average Delay

6. Conclusion

The Dynamic Load Balancing Privacy Path Selection (DLBPS) algorithm evaluated and analyzed for mobile ad hoc networks on the strength of packet transmission and attack prevention. The DLBPS method performs gateway mobility load balancing in the network order to achieve higher aggregated throughput among data transfer. Meanwhile, the proposed algorithm establishes detection, privacy collector privacy manager and privacy propagator to complete the privacy path selection. An experimental result shows that the proposed algorithm performs better than existing HsecGR and Trust-ECC methods3

References

1. Jayaprakash.R., and Radha,B., : CBPPRS: Cluster Based Privacy Preserving Routing Selection in Wireless Networks, International Journal of Engineering & Technology, Vol. 7 (3.12) (2018) 439-443
2. Jayaprakash.R., and Radha,B., : LBCPR: Load Balancing Cluster Based Privacy Routing In Wireless Networks, International Conference on Recent Trends in Automation (ICRTA-2018)
3. Chatterjee, M., SK Das., Turgut,D., : WCA: a weighted clustering algorithm for mobile ad hoc networks. Clust. Comput., Kluwer Adademic Publishers, Manufactured in The Netherlands, Vol. 5 (2002) 193-206

4. Bednarczyk, W., Gajewskil,p., : An enhanced algorithm for MANET clustering based on weighted parameters. Universal J. Commun. Netw. Vol. 1(3) (2013) 88–94
5. Ephremides., Jeffery Wieselthier., Dennis Baker., : A Design Concept forReliable Mobile Radio Networks with Frequency Hopping Signaling. Proceedings of the IEEE Vol. 75,No. 1, (1987) 56-72
6. Gupta, A.K., Sadawarti, H., Verma, A.K.,. : Review of various routing protocols forMANETs. Int. J. Inf. Electron. Eng. Vol. 1(3), (2011) 251–259
7. Kaur, H., Singh, H., Sharma, A.: Geographic routing protocol: a review. Int. J. Grid Distrib. Comput. Vol. 9(2), (2016) 245–254
8. Sarika, S., Pravin, A., Vijayakumar, A., Selvamani, K.: Security issues in mobile adhocnetworks. Procedia Comput. Sci. Vol. 92, (2016) 329–335
9. Boulaiche, M., Bouallouche-Medjkoune, L.: Hsecgr: highly secure geographic routing. J. Netw. Comput. Appl. Vol. 80, (2017) 189–199
10. Kaur, M., Kaur, S.: Analyze and implementation of cluster based routing protocol inMANETs. Int. J. Innov. Res. Sci. Eng. Technol. Vol. 5(3), (2016) 3098–3107
11. Rajasekar, S., Subramani, A.: Performance analysis of cluster based routing protocol For MANET using RNS algorithm. Int. J. Adv. Res. Comput. Sci. Softw. Eng. Vol. 6(12), (2016) 234–239
12. Boulaiche, M., Bouallouche-Medjkoune, L.: Hsecgr: highly secure geographic routing. J. Netw. Comput. Appl. Vol. 80, (2017) 189–199
13. S. Syed Jamaesha and S. Bhavani, A secure and efficient cluster based location aware routing protocol in MANET, Springer Science+Business Media, LLC, part of Springer Nature 2018.

Chapter - 06

A TRUSTED KEY MANAGEMENT PROTOCOL (TKMP) FOR CLUSTER BASED WIRELESS NETWORKS

Abstract: One of the protected communication techniques in cluster based privacy preserving MANET is providing a Trusted Key Management Protocol (TKMP). A TKMP calculates a trust key exchanging for all the cluster nodes in the communication for security. TKMPallocates a dynamic private and public key exchanging value for trust variable where it will be checked during communications.The total proposed protocol is executed in three stages, for example, Initial-sending, key creation and validation of key and affirmation. In the primary stage, the cluster nodes are offered with the unique identity (ID), and after that, the following stage utilizes the Paillier cryptosystem (PC) holomorphic encryption model, for making the basic key to the message correspondence. Finally, a geometrical model is created in this work with various variables, for example, a hashing capacity, homorphic encryption, profile succession, irregular number capacities. The proposed TKMP strategy sets up the verified correspondence over the WSN by the authentication process.

Keywords: Cluster Network, Secured Communication, Key development, Key Validation, Homomorphism Encryption

I. INTRODUCTION

The Mobile Adhoc Network is a division of Wireless Sensor Network but MANET is ad-hoc in nature. Every node can be initialized, formed, stimulated, disabled and become dead at all time anywhere in the network. In case of MANET which is dynamic and based on the concept of clustering, the functions of the node are not only acting as terminals end and also as a router in-between. Data packets sent by an origin node can attain to a target node through an amount of hops i.e. more than single node capacity be concerned in forwarding messages from origins to targets. MANET succeeds to exclusive privacy preserving properties such as random and dynamic network topology, random mobility and less wireless relations. These properties carry several considerable technical challenges of Quality of Service (QoS) control, routing and security. A hand full of research has been done for the development of the Quality of Service and for the privacy preserving inside the clusters in a MANET. For the security of a cluster to be affordable, all the MANET need to acquire a security necessities in line with the accessibility provision , preserved privacy , truth , a valid verification and the non-redundant[3] .

The cluster based models for the security in case of a MANET are then suffering from various kind of security breaches that can be approached from the external nodes that are malicious and also compromised MANET nodes.[3,4]. For the protection of routing kind of information, the packets are then coded using a particular key technique [5-7]. The secure cluster based routing protocol had been compatible with some additional reactive routing based protocols was establish to be protected to the attacks that could interrupt the procedure to route discovery. This allows the identification of routes based hotspot for evacuation the deceptive reacts and such secure directing conventions will depend totally on the security relationship among the starting point and the objective hub. The security relationship may likewise be made by assets of utilizing a portion of a blend key that has been founded on that of the open keys of a root hub (O) and furthermore an objective hub (T). The O and the T will utilize a mystery symmetric key which is the (KeyO ,T) that utilizes the open keys of one another.

In the paper, we developed a novel secure routing key management scheme based on Trusted Key Management Protocol (TKMP) is authenticating the public and private key encryption and decryption algorithm is used in protecting the packets or messages from attackers in this phase. In the next section, recent studies for public key development methods are presented and concepts are given. In section 3, our proposed TKMP model is presented where a new trust key model is introduced and verification processes are described. Finally, conclusion remarks are given in the last section.

II. BACKGORUND STUDY

(*Azarderakhsh, Reza, ArashReyhani-Masoleh, and Zine-EddineAbid*, **2008**)[8] stated that the key management in cluster-based wireless sensor networks using both private and public key cryptography. Their objective is to introduce a platform in which public key cryptography is used to create a secure path among sensor nodes and gateways. Instead of pre-loading a huge amount of keys into the sensor nodes, every node desires a session key from the gateway to set up a secure path with its neighbors after clustering phase. The security examination and performance evaluation showed that the key management method has considerable saving in storage space, broadcast overhead, and perfect resilience against node capture.

(*Udaya, D., SuriyaRajkumar, and RajamaniVayanaperumal*, **2013**) [9] examined a security is one of a significant factor to be viewed as truly in remote sensor systems. In WSN, from multiple points of view interruption may happen, in the history decades there is no ideal IDS, with no squandering of assets like time, vitality, cost and number of physical things. The principle target is to guarantee the security and improve the nature of system by applying a Leader based interruption identification framework in the Wireless Sensor Network (WSN). Here, we are concentrating on the assault known as sinkhole assault which is considered as the greatest risk in remote sensor organize which crown jewels the total correspondence and an information misfortune between a couple of hubs as source hub and a goal hub. So as to give a total answer for identify and dodge sinkhole assault a Leader Based Intrusion Detection System (LBIDS) is proposed. Their methodology a pioneer is chosen for each gathering hubs inside the system, area savvy and it do looks at and figures the conduct of every hub, intelligently executes our identification module and screens every hub conduct inside the bunch for any sinkhole assault to happen.

(*Xun Yi, Russell Paulet, Elisa Bertino*, **2014**) [10] considered the issue that includes executing an encoded focused on commercial framework that creates ads relying upon the substance of a client's email. Since the email is put away in an encoded structure with the client's open key, the email server plays out a homomorphic assessment and processes a scrambled notice to be sent back to the client. The client unscrambles it, plays out an activity relying upon what she sees. On the off chance that the commercial is significant, she may tap on it; else, she just disposes of it. Be that as it may, if the email server knows to this data, to be specific whether the client tapped on the ad or not, it can utilize this as a confined unscrambling prophet to break the security of the client's encryption plan and conceivably considerably recoup her mystery key. Such assaults are omnipresent at whatever point we figure on encoded information, nearly to the point that CCA security appears to be inescapable. However, it is anything but difficult to see that picked ciphertext (CCA2-secure) homomorphic encryption plans can't exist. In this way, a suitable security definition and developments that accomplish the definition is sought after.

(*Q. Jiang, S, Zeadally,J. Ma and D. He*,**2017**) [11introduced a lightweight and secure client verification convention dependent on the Rabin cryptosystem, which has the highlights of computational asymmetry. They led a perceived affirmation of the convention utilizing ProVerif so as to display that the strategy finishes the vital security properties. The creators introduced a total heuristic security examination to demonstrate that the convention is secure next to all the potential assaults and gives the ideal security highlights.

(*Razaque, Abdul, and Syed S. Rizvi*, **2017**) [12]expressed that the past secure information collection approaches for remote sensor systems were not proposed for consent, vitality productivity and proper security, leaving them inclined to assaults. The creators presented the protected information accumulation utilizing the entrance control and validation (SDAACA) convention. Utilizing SDAACA convention to see sinkhole and Sybil assaults that are hard to distinguish by existing cryptographic methodologies. The SDAACA convention comprises of two novel calculations: the protected information fracture (SDF) and the hub blend approval (NJA). The SDF calculation secretes the information from the foe by dividing it into little pieces. In the

NJA calculation, an approval procedure is started previously enabling any new hub to join the system. The two calculations help improve the Quality of Service (QoS) parameters

(*Jaewoo Choi, Jihyun Bang, LeeHyung Kim, MirimAhn, and Taekyoung Kwon*, **2017**) [13] proposed an area based key administration plot for WSNs, with uncommon thought of insider dangers. In the wake of surveying past area based key administration strategies and examining their benefits and negative marks, they chose area ward key administration (LDK) as an appropriate technique for their investigation. To unravel a correspondence impedance issue in LDK and comparable strategies, they have concocted another key update process that consolidates matrix based area data. They likewise proposed a key foundation procedure utilizing network data. Besides, they developed key update and denial procedures to adequately oppose inside aggressors. For examination, led a thorough reenactment and affirmed that their method can intensify network while diminishing the trade off proportion when the base number of normal keys required for key foundation is high.

(*Ahlawat, Priyanka, and Mayank Dave*, **2018**) [14]Talked about to diminish the hub catch crash by consolidating a productive antagonistic model for cell model of WSN. The antagonistic model builds up various vulnerabilities introduced in the system, for example, raised hub thickness, task of the sink hub, neighbor weight factor to ascertain the arrangement likelihood of every cell. It at that point depicts the hash chain length for each cell with different rekey period to intensify the system obstruction against hub catch assault. Their technique is contrasted and different past strategies regarding the probability of key trade off and the measure of ways rekeyed. The results affirm its viability in expanding the WSN security.

III Trusted Key Management Protocol (TKMP)

The proposed TKMP significant goal is to structure and build up a dynamic key administration based protocol dependent on normal and staggered verification in Clusters. The proposed convention includes three units, for example, Cluster Head (CH), Cluster Member (CM), and base station (BS) for the key organization in the system. The general arrangement of the proposed TKMP incorporates the accompanying three stages, for example, Initial-sending, key creation, and key approval and validation. In the primary stage, the bunch part hubs in the system are given the one of a kind personality, and in the key creation stage, lightweight key creation dependent on upgraded homomorphic encryption is utilized to produce the keys. Ultimately, the key approval and check are finished by determining a geometrical model utilizing a hashing capacity, improved homomorphic encryption, irregular number capacities. In this way, with the created geometrical model for the key advancement, the proposed TKMP validates the units and accordingly, manages a protected and dynamic key improvement in the bunched Network. The figure 1 portrays the TKMP procedure stream.

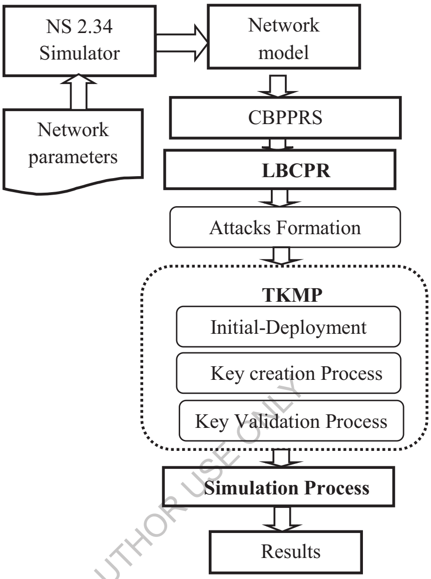


Fig.1: TKMP process Flow

Network Architecture

Network model contains of *M* number of nodes deployed randomly within network simulation area. All the nodes (N(k)) are dynamic in terms of their creation, location and lifeless. Apart from all the general nodes, the cluster network has two well-configured nodes called as the base station (B_{st}) and Cluster Head (CH). The behaviours of the whole mobile nodes are observed, record and pass it to B_{st} is carried out by the CH. The network formation is evaluated in graph model was already we presented (*R. Jayaprakash*, *B. Radha*, **2018**). The current network includes of Cluster Member (CM) is assigned a unique ID for validation and authorization. Any *N*(*k*) can broadcast the packets to any other *N*(*l*)) in the network without any restrictions (*R*(*k*)). All the nodes can modify their location dynamically. In order to provide secure communication, each node is verified using their ID for authenticating and authorizing for communicating with other nodes in the network.

CBPPRS and LBCPR

Cluster Based Privacy Preserving Routing Selection (CBPPRS) was at that point we exhibited (R. Jayaprakash, B. Radha, 2018) thinks about the gathering of Cluster heads (CH) in a portable ado system of n intersections/hubs to such an extent that all hubs in this system are inside separation h jumps of a CH, for a known DEFINED – VALUE.

The Load Balancing Cluster Based Privacy Routing (LBCPR) was already we presented (*R. Jayaprakash*, *B. Radha*, **2018**) load awkwardness in the system and the inclination or bias in getting halfway found hubs for information move. The proposed a novel group based directing measurement, load and a minimization rule to settle on a choice a way that involves versatile hubs with less burden weight on them In LBCPR performs new measurement called burden will reveals to us the evaluated burden a portable hub (mn) is engaged to in a system, its worth will indicate the evaluate of current burden. In this model, connect looking and send react calculations performs bunch burden field precisely.

Attacker Model

In the model for attacker, The following are done

1. The Attacker is able to capture all of the traffic in the area of network concerned.
2. The snooping is so promising in the network and the communications and of the knowledge on the nodes that are nearby following the message size , etc
3. Depending on the variation, there seems to be certain possibilities in the attack that drops the packets into the network.

TRUSTED KEY MANAGEMENT PROTOCOL (TKMP)

This part depicts the proposed TKMP, for making a verified correspondence interface in clustered Network. The proposed TKMP performs key advancement in three unique stages. The development of TKMP is portrayed in figure 2. As exhibited in the above figure, the TKMP three stages are 1) Intial-Deployment, 2) Key Creation, and 3) Key Validation and Confirmation. The proposed TKMP can be estimated as the advancement to the Paillier cryptosystem (PC), with the end goal that utilizes the open key for secure correspondence. The means engaged with the proposed TKMP are advised as pursues:

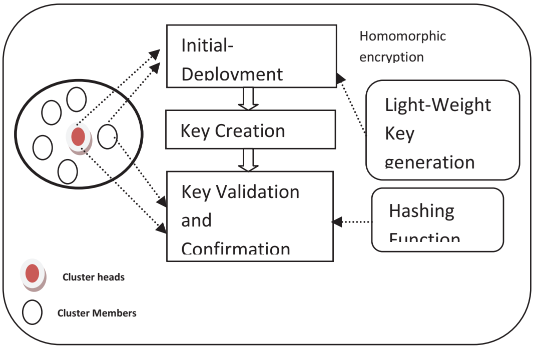


Fig. 1: TKMP Architecture

a) Initial-Deployment Phase

The first process in the proposed TKMP is the Intial-arrangement stage, where the portable hubs are given a specific personality (ID). Ordinarily, this stage allots the doable recognizable proof for each group part (CM) hub, BS, and CHs. As the CH is one of the key needs in remote system correspondence, the Initial-arrangement is done after the creation grouping Network portable hubs. Subsequent to bunching the system model, various CHs are shaped.

The Initial phase fills the predefined network key N_{key} to every node, CH and BS in the wireless network. The cluster based wireless network has its parameters for everybeginning of communication. Most of the network uses the network key of 128 bits for secured transmission. The paper adopts the homomorphic encryption [22] for creating the network key.

b) Key Creation Process

After given that the personality for the group hubs, the following most significant stage is to make key for CM, CH and BS. The key creation stage helps with delivering the private and the open keys for the correspondence in the midst of the versatile hubs. This paper acknowledges the PC Encryption Scheme inferred in [22] for making the private and the open keys for the portable hubs. The means received by PC technique for key age are clarified as pursues:

Consider the k^{th} mobile node in cluster network which starts the correspondence and it needs both the open key and the private key for the correspondence reason. Basically, the root hub makes two separate enormous prime numbers p and q. At that point, the creation$C = pq$ is calculatedamong the random numbers p and q. The private key λ is determined using Carmichael‘s function,

$$\lambda(n) = lcm(p-1)(q-1) \quad \text{eqn. (1) ,The rest factoris calculated as,}$$

$$r_p^{(p-1)/2} = -1(modp)\ r_q^{(q-1)/2} = -1(modp) \quad eqn.\ (2)$$

Public Key Generation: For creating the public key, the rest factor r and the product C are used. Thus, the public key consists of (r, C).

Private Key generation: The private key is constructed based on (p, q).

The above steps are applied for creating the private and the public keys for the CM, CH and BS. The key created for CM, CH and BS is given as follows:

$$[CM^{r}{}_{key}, CM^{P}{}_{key}] = \mathrm{PC}(p_1, q_1) \quad eqn.\ (3)$$

$$[CH^{r}{}_{key}, CM^{P}{}_{key}] = \mathrm{PC}(p_2, q_2) eqn.\ (4)$$

$$[BS^{r}{}_{key}, BS^{P}{}_{key}] = \mathrm{PC}(p_3, q_3) eqn.\ (5)$$

Equation (3) represents the Cluster Member (CM), equation (4) for Cluster Head (CH) and equation (5) for Cluster Head (CH). Where, (p_1,q_1), (p_2,q_2) and (p_3,q_3) are group of large distinct prime numbers stated for the CM, CH and BS, respectively.

C) Key Validation and Confirmation Process

The last phase in the proposed TKMP is the validation and confirmation of the key. This stage exhibits the progression of communication in the midst of the origin and the objective versatile cluster in the validation of the key and affirmation stage. Preceding exchange a verified packet over the correspondence arrange, it is basic to make a secured path for communication among the CM. The secured path for communication is outstanding among the sender and the beneficiary in the key approval stage, in front of moving the parcel. For each datum transmit, the TKMP makes the session key, to find the cipher text.

Begin the data transmit: The packet transmits is started by the origin node and the packet has its individual identity (ID), network key (N_{key}), and code.

$$APK_{xy} = \begin{bmatrix} Enc(Pid) & Enc(Rid) & Enc(Sh^{xy}_{jey}) \\ Message & Message & Message \end{bmatrix} \begin{cases} Packet_1 \\ Packet_2 \\ Packet_M \end{cases} \quad eqn.(6)$$

where, *Pid* indicates the packet identity, *Rid* indicates the identity of the receiver node and $Sh^{xy}{}_{key}$ refers to the shared key createdamong the origin and the target node. The function *Enc*()determines the encryption, which is finished utilizing the improved PC calculation with the help of the session key session+key. The session key is one of the noteworthy components in the proposed TKMP. The session key is made temporarily, which lives for the message session done during the information transmit between the hub x and y. The accompanying articulations demonstrate the encryption done through the improved PC technique.

$$\text{Enc}[P_{id}]= PC(P_{id}, \text{session}^{+}{}_{key}) \quad eqn.\ (7)$$

$$\text{Enc}[R_{id}]= PC(R_{id}, \text{session}^{+}{}_{key}) \quad eqn.\ (8)$$

$$\text{Enc}[Sh_{id}] = PC(Sh^{xy}{}_{key}, \text{session}^{+}{}_{key}) \quad eqn.\ (9)$$

After the achievement of the session key through the sender, the organization is done by the receiver which recognizes the origin which tries to communicate through the secured link of communication. The TKMP executes the parcel move just driving building up the verified information way (connect). For this kind of message, the recipient confirms the specialist of the starting point by making ciphertext. Essentially, the collector makes the ciphertext C1. The ciphertext C1 is accomplished dependent on the center bundle MP. The center bundle MP relies upon the unscrambled data with the session key, and it relies upon the accompanying condition,

$$MP = \begin{bmatrix} Dec(Enc(Pid)|session^{+}_{key}\,(recevied)| \\ \Big(Enc(Rid)|session^{+}_{key}\,(recevied)\Big|||Dec(Enc(Pid)|Sh^{xy}_{key}\,(received))\Big) \end{bmatrix} \quad eqn.(10)$$

Where, session^{+}($received$) refers to the session key established by the receiver, and *Dec*() specifies the decryption done on packet entities based on the received session key.

Generation of ciphertextC_1 and C_2 can be referred as the security layer 1.

$$C_1 = \ hash(MP) \quad eqn.\ (11)$$

The ciphertextC_2 is created based on the ciphertextC_1. The next security layer is awarded by the network key, and thus, the ciphertextC_2 is created as follows,

$$C_2 = [Dec(Enc(C_1)|N_{key})||CH^p{}_{key}] \quad \text{eqn. (12)}$$

$$C^*{}_2 = [(Enc(C_1)|N_{key})||CH^p{}_{key}] \quad \text{eqn. (13)}$$

After creating C_2, the receiver replies the sender ask for by transfer the ciphertextC_2.Clearly the TKMP acknowledges the parcel during staggered security level, and in this way, diminishes the opportunity of security robbery. The sender confirms the honesty of the collector by indistinguishable the determined ciphertext C2∗ with the ciphertext built up from the beneficiary C2. Once together the ciphertext matches, for example C*2 =C2, the sender announces the beneficiary to be reasonable and accordingly, starts the first information transmit. On the off chance that the figure does not coordinate, the message will be ended, and the session key made for the message gets terminated.

Algorithm 1: *TRUSTED KEY MANAGEMENT PROTOCOL (TKMP)*

```
Intialize CH,CM,BS.

Process

Step 1: Allocate $N_{key}$ to CM, CH and BS using improved PCalgorithm.

Step 2: For each CM, CH and BS and Generate Key Creation using equation 3,4 and 5

        End for

Step 3: Execute encryption above the $P_{id}$, $R_{id}$, and Shared key

Step 4: Start packet transmission and updates Active Profile Key using eqn, (6)

Step 5: Calculate Cipher Text using eqn. (11) & (12)
Step 6: Origin Node finds $has(MP*)$ and $C_2*$ correspondingly.
Step 7: if$C_2* = C_2$ then
Start packet transfer
else
        State the $y_{th}$ mobile node as the malicious
endif
```

CONCLUSION

The main objective of this paper is to provide a Trusted Key Management Protocol (TKMP) to improve the quality of secure communication in Cluster based Wireless network. The TKMP is explicitly intended for the grouped system, and it has three phases, in particular Initial-arrangement, key creation and key approval and affirmation. The proposed TKMP performs Paillier cryptosystem (PC) homomorphic encryption is accomplished for disclosure the encryption key. In the interim, the proposed calculation builds up geometrical model created with the verified variables, for example, hashing capacity, homomorphic encryption, profile key succession, irregular number capacities for verified data transmission.

REFERENCES

[16] R. Jayaprakash and B. Radha ,"CBPPRS: Cluster Based Privacy Preserving Routing Selection in Wireless Networks", International Journal of Engineering &Technology, 7 (3.12) (2018) 439-443.

[17] R. Jayaprakash and B. Radha ,"LBCPR: Load Balancing Cluster Based Privacy Routing In Wireless Networks", International Conference on Recent Trends in Automation (ICRTA-2018).

[18] L. Zhou, Z. J. Haas, "Securing ad hoc networks", IEEE Network, Vol. 13, No. 6, Nov. 1999, pp: 24 – 30

[19] Y. C. Hu, A. Perrig, "A survey of secure wireless ad hoc routing", IEEE Security & Privacy Magazine, Vol. 2, No. 3, May-June 2004, pp: 28 - 39

[20] Y. C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks", in the Proc. Of 8th Annual International Conference Mobile Computing and Networking (Mobicom 2002), ACM Press, 20002, pp. 12-23

[21] M. G. Zapata, N. Asokan, "Securing ad hoc routing protocols", in the Proc. Of ACM Workshop on wireless security (WiSe), ACM Press, 2002, pp: 1-10

[22] K. Sanzgiri et al., "A secure routing protocol for ad hoc networks", 10th IEEE International Conference on Network Protocols, 2002, 12-15 Nov. 2002, pp: 78 - 87

[23] Azarderakhsh, Reza, Arash Reyhani-Masoleh, and Zine-Eddine Abid, "A key management scheme for cluster based wireless sensor networks," Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, pp. 222-227, 2008.

[24] Udaya, D., Suriya Rajkumar, and Rajamani Vayanaperumal, A leader based monitoring approach for sinkhole attack in wireless sensor network, J. Comput. Sci., 2013, vol. 9, no. 9, pp. 1106–1116.

[25] Xun Yi, Russell Paulet, Elisa Bertino, "Homomorphic Encryption and Applications," Springer Briefs in Computer Science, 2014

[26] Q. Jiang, S, Zeadally, J. Ma and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," in IEEE Access, vol. 5, pp. 3376-3392, 2017.

[27] Bhajantri, Lokesh. (2018). A Comprehensive Survey on Data Aggregation in Wireless Sensor Networks. International Journal of Computer Sciences and Engineering. 6. 798-802. 10.26438/ijcse/v6i7.798802..

[28] J. Choi, J. Bang, L. Kim, M. Ahn and T. Kwon, "Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks," in IEEE Systems Journal, vol. 11, no. 2, pp. 494-502, June 2017.doi: 10.1109/JSYST.2015.2422736

[29] Priyanka Ahlawat, Mayank Dave,An attack model based highly secure key management scheme for wireless sensor networks, Procedia Computer Science,Volume 125,2018,Pages 201-207,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2017.12.028.

Chapter - 07

IDENTITY BASED CRYPTOGRAPHY AND IMPLEMENTATION IN MANET

Since Identity-Based cryptography was proposed and came true in 2001, many researchers have been conducted to apply the new technology to MANETs. In the literature, the application covers key management, improvement of PKIs, secure communications, secure routing protocols, and some other topics of MANETs. In the following section, we study the application of Identity-Based cryptography in these areas of MANETs.

Key Management using Identity Based Cryptography

A basic key generation scheme of Identity-based Cryptography has been present in [Boneh and Franklin 2001]. To scale to a large network of users and secure the key generation process, some key generation schemes have been proposed.

A new secure key issuing protocol in which a private key is issued by a key generation center (KGC) and then its privacy is protected by multiple key privacy authorities (KPAs). For all i = 1, · · ·, n, KPA_i chooses his master key si and computes his public key $P_i = s_iP$. Then KPAs cooperate sequentially to compute the system public key $Y = s_0s_1...s_nP$. A user ID gets its private key in three stages.

1. In key issuing stage, a user with identity ID sends his identity ID and blinding factor $X = xP$ to the KGC and requests him to issue a partial private key. Then, after checking the identity of the user and computing the public key of the user – Q_{ID}, the KGC issues a partial private key to the user in a blinded manner: $Q'_0 = H_3(\hat{e}(s_0X, P_0))s_0Q_{ID}$, together with a signature: $Sig_0(Q'_0) = s_0Q'_0$. Here $H_3(\hat{e}(s_0X, P_0))$ is a blinding factor; a secure channel between the user and the KGC. User can unblind it using his knowledge of x, since $H_3(\hat{e}(s_0X, P_0)) = H_3(\hat{e}(s_0xP, P_0)) = H_3(\hat{e}(P_0, P_0)_x)$.
2. In key securing stage, the user requests multiple KPAs in a sequential manner to provide key privacy service by sending ID, X, Q'_{i-1} and $Sig_{i-1}(Q'_{i-1})$. Then KPAs return the private key shares: $Q'_i = H_3(\hat{e}(s_iX, Pi))s_iQ'_{i-1}$ and signature $Sig_i(Q'_i) = s_iQ'_i$ in a blinded manner.
3. Finally, in key retrieving stage, the user unbinds it to retrieve the real private key: $D_{ID} = Q'n\, H_3\, (\hat{e}\,(P_0, P_0)\, x) \cdots H_3\, (\hat{e}\,(Pn, Pn)\, x) = s_0s_1 \cdots snQ_{ID}$. The user can verify the correctness of his private key by $\hat{e}\,(D_{ID}, P) = \hat{e}\,(Q_{ID}, Y)$.

Preliminaries of Key management in MANET

Key management must solve the problem of sharing a secret among a number of users. To identifies the problem of how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces [1], but even complete knowledge of k − 1 pieces reveals absolutely no information about D.

In the proposed scheme, a (k, n) threshold scheme to solve this problem based on polynomial interpolation: given k points in the dimensional plane (x_1, y_1)...... (x_k, y_k), with distinct x_i's, there is one and only one polynomial q(x) of degree k – 1 such that $q(x) = y_i$ for all i. To divide the secret D into n pieces, he suggests picking a random k − 1 degree polynomial $q(x) = a_0 + a_1x + \cdots + a_{ki}x_{k-1}$ in which $a_0 = D$, and each piece is the value of the polynomial at the n points: $D_1 = q(1), \cdots D_i = q(i), \cdots, D_n = q(n)$. Thus any subset of k of the pieces can determine the coefficients of the polynomial (using e.g. Lagrange interpolation) and thus the secret data at a certain point. To make this claim more precise, he suggests the use of modular arithmetic instead of real arithmetic. The set of integers modulo a prime number p forms a field in which interpolation is possible. This scheme was later referred to many times to construct a distributed PKG in Identity-Based cryptography and to solve security problem in ad hoc networks.

This scheme was later referred to many times to construct a distributed PKG in Identity-Based cryptography and to solve security problem in ad hoc networks.

Identity Based Cryptography from bilinear pairings

This is no longer a problem in identity-based cryptography, since now the public key of each user can be derived, in a public and efficient way, directly from his identity (e.g. e-mail address, IP address, etc.). Therefore, the link between identity and public key is established for free, from the beginning. Later, the user must contact some master entity in order to obtain his secret key. The master entity has his own pair of secret/public keys, and uses his secret key to compute the secret keys of the users. The main drawback of this paradigm is that the master entity knows the secret keys of all the users.

Most of the identity-based cryptographic schemes which have been proposed up to now employ bilinear pairings, which are maps e: G X G → G_T, for groups G (additive) and G_T (multiplicative) of the same prime order q, with the following properties:

1. Bilinear: e (aP, bQ) = $e(P,Q)^{ab}$, for all P,Q € G, a, b € Zq.
2. Non-degenerate: e(P, P) ≠ 1_{GT} for all P € G.
3. Computable: there exists an efficient algorithm to compute e(P,Q) for any P,Q € G.

Setup

An additive group G of prime order q (generated by some public element P) and a multiplicative group GT of the same order are chosen admitting a bilinear pairing e: G X G → GT. Three hash functions H_1: {0, 1}* → G, H_2: GT → $\{0, 1\}^1$ and H_3: G X $\{0, 1\}^1$ → G are needed, where l is the bit-length of the messages to be encrypted.

The master entity has a secret key s € Zq which is chosen at random; the matching master public key is the element PK = sP € G.

Key Generation

Assume that the group SG has n users, SG = {P_1, . . .,P_n}. Let t^1 be the decryption threshold such that 1 ≤ t^1 ≤ n. If IDSG is the public identifier of the group, then the master entity first computes the matching secret key SK_{SG} of the group as SK_{SG} = sH_1 ($ID_{SG)}$ € G. Then, he picks R_1, . . ., $R_t^1$0-1 at random from G, and defines the mapping

$$R(z) = \mathrm{SK}_{\mathrm{SG}} + zR_1 + \cdots + z^{t'-1}R_{t'-1} \in \mathbb{G},$$

Where the variable z takes values in Zq. Each user Pi € SG is (publicly) assigned to a different value zi € Zq.

Encryption

Given a message m € $\{0, 1\}^1$ to be encrypted and addressed to the group SG, the sender chooses uniformly and at random r € Zq. Then he computes the value $K = e(PK, H^1(ID_{SG}))^r$ and the triple of values $U = rP$, $V = H_2(k)$ ¤ m, $W = rH_3(U,V)$ which define the resulting ciphertext C = (U,V,W).

Threshold Decryption

Given a ciphertext C = (U, V, W), a member P_i € SG of the group can use his secret share $[SK_{SG}]_i$ to compute a partial decryption, as follows. First of all, he checks if e (P, W) = e (U, $H_3(U,V)$).

Identity Based Cryptography & its Methodology

This scheme achieves an extremely self organized behavior by simply giving the security settings of each node to itself [2]. The approach uses trust graphs in place of the certification graphs as proposed in. These graphs are similar to small worlds in PGP. Thus, the trust relationships formed by mobile ad hoc network members must exhibit the same features as PGP system. The major goal of the proposed scheme is to provide a secure environment to send the messages from source to destination. The source will decide the route based on the trust graph which is constructed on its own. The source will encrypt the message that will be decrypted at destination only. However, the source will not allow decrypting the message either by intermediate node or by any other intruder. The following are the basic operations for implementation of the scheme. Initial phase of the proposed scheme is executed in four steps.

Step 1: Generate the public-private key pairs.

Step 2: Send the generated public key to neighbors, and wait for reply messages.

Step 3: Receive the neighbor public keys and send reply messages.

Step 4: Send the self signed certificates encrypted with neighbor's public keys to those are whom it has received their public keys. Wait for reply message that can be decrypted with its own private key.

Step 5: Receive the certificates from the neighbors, decrypt them and store in certificate repository (CR1) and then, send replies encrypted with their public key.

Step 6: Send the key repository to its neighbor, each node will send encrypted destination certificate and the repository will be encrypted with public key of destination.

Step 7: Receive the key repository and decrypt it with its own private key and authenticate the message digest with destination public key, update the own shared repository and trust graph with this new update.

Step 8: Send the updated self signed certificate encrypted with the public key of destination and attached with the valid certificate of destination.

Step 9: Send the updated public key to neighbors encrypted with the destination public keys and the digest with the old private key, to allow the destination to decrypt the message with existing public key of sender.

Step 10: Receive the revoked certificates of neighbors and authenticate the message with valid existing certificate and public key.

Step 11: Receive the revoked public key and authenticate the message with existing certificate and public key. And update own shared repository and in turn send the revoked public key and trust graph to their neighbors other than the sender.

Step 12: Compose the message at source with destination address and the required message, encrypt the message with a symmetric key (SK1) generated for that message and the digest with its own private key.

Step 13: Find the efficient route based on the trust graph considering the shortest path and expire times of the router.

Step 14: Encrypt the route and the neighbor certificate with another symmetric key (SK2) and digest with its own private key. And the SK2 will be encrypted with neighbor’s public key.

Step 15: Attach the main message composed in Step 12 with the message (route and certificate) composed at Step 14, send it to the neighbor.

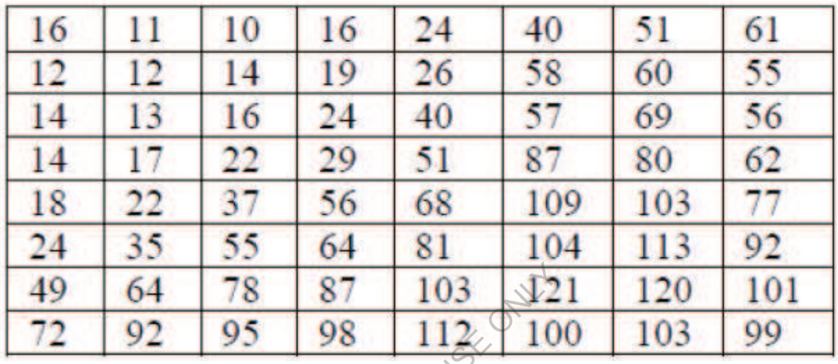
Step 16: Receive the message from the neighbor and decrypt the session key with its own private key and get the symmetric key (SK2) and decrypt the message (route and certificate), find whether the destination in the route path is the node itself or other. If the message was supposed to the node itself, then authenticate the certificate and decrypt the main message asymmetric key (SK1) with its own private key; otherwise direct the message to its neighbor (based on route) by adding certificate and route path.

The encoding and decoding process of the cryptography method is illustrated below.

Quantization is the procedure of constraining something from a relatively large or continuous set of values (such as the real numbers) to a relatively small discrete set (such as the integers. The discrete cosine transform (DCT) helps separate the text into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform but it use only real numbers. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT"; its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transforms (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transforms (MDCT), which is based on a DCT of overlapping data.

The most powerful and quantization technique used for the cryptography is vector IBC. The IBC uses vector quantization algorithms for reducing the transmission bit. Text vector quantization algorithm includes four stages: vector formation, Training set selection, codebook generation and quantization. The first step is to divide the input into set of vectors. The Subset of vectors in the set is later chosen as a training sequence. The codebook of code words is obtained by an iterative clustering algorithm. Finally, in quantizing an input vector, closest code words in the codebook is determined and corresponding label of this code word is transmitted. In this process, data compression is achieved because address transmission requires fewer bits than transmitting vector itself. The concept of data quantization is extended from scalar to vector data of arbitrary dimension. Instead of output levels, vector quantization employs a set of representation vectors (for one dimensional case) or matrices (for two dimensional cases). Set is defined as ―codebook‖ and entries as ―code words. Vector quantization has been found to be an efficient coding technique due to its inherent ability to exploit the high correlation between the neighboring pixels

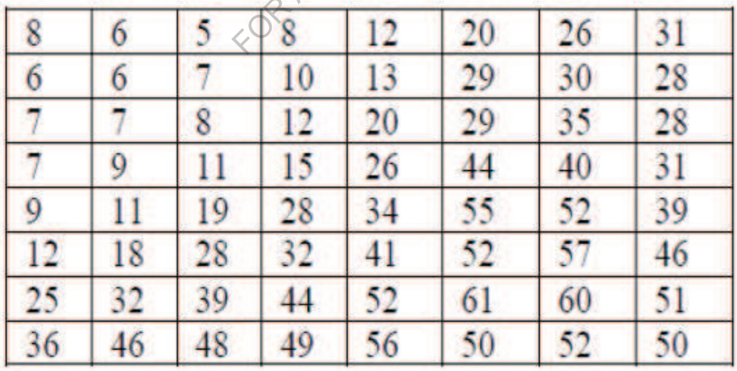
JPEG technique divides the input image into non-overlapping blocks of 8x8 pixels and uses the DCT transformation. For each quantized DCT block, the least two-significant bits (2-LSBs) of each middle frequency coefficient are modified to embed two secret bits. Using gray-level cover images, we transformed (DCT) non-overlapping blocks of 16x16 pixels instead of non-overlapping blocks of 8x8 pixels. The transformed DCT coefficients were quantized by a modified 16x16 quantization table. Then, we embedded the secret data within the middle frequency coefficients



16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

8 X 8 quantization table

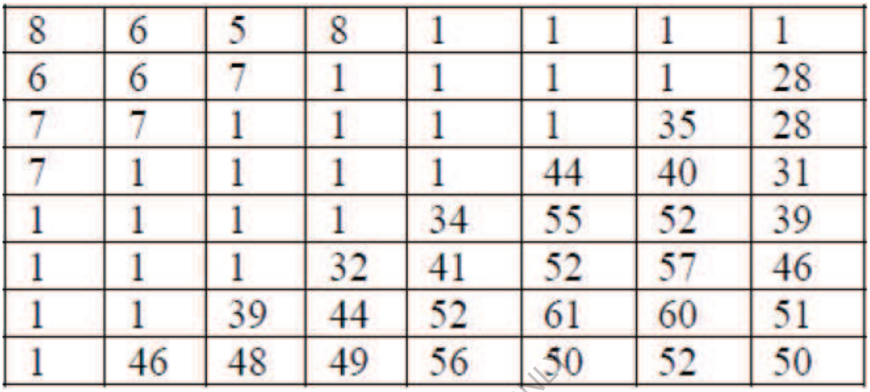
Dividing this quantization table and by 2, we can get a new quantization table, like below.



8	6	5	8	12	20	26	31
6	6	7	10	13	29	30	28
7	7	8	12	20	29	35	28
7	9	11	15	26	44	40	31
9	11	19	28	34	55	52	39
12	18	28	32	41	52	57	46
25	32	39	44	52	61	60	51
36	46	48	49	56	50	52	50

The scaled quantization table

Using this new quantization table generates reconstructed images almost identical to the source image. The modified version of (Table II), has been used within Chang et al. method. 8x8 quantization tables apart, there are no samples for larger quantization tables in the JPEG standard

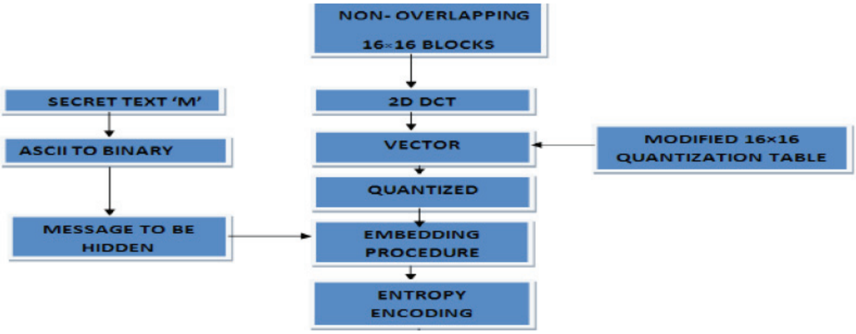


8	6	5	8	1	1	1	1
6	6	7	1	1	1	1	28
7	7	1	1	1	1	35	28
7	1	1	1	1	44	40	31
1	1	1	1	34	55	52	39
1	1	1	32	41	52	57	46
1	1	39	44	52	61	60	51
1	46	48	49	56	50	52	50

Modified quantization table

Encoding Steps: -

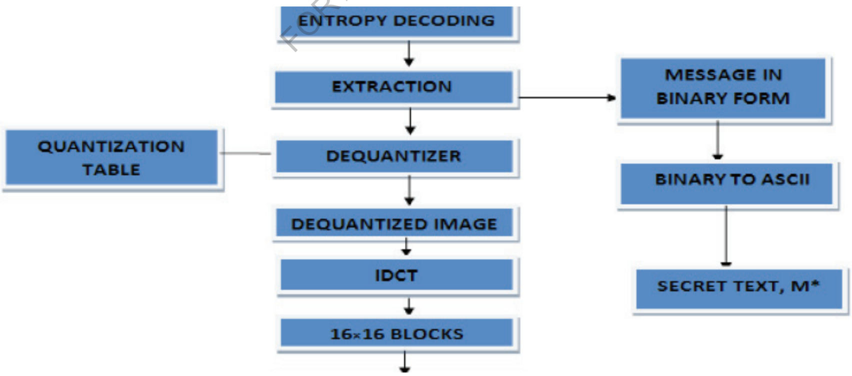
- A cover image of any size and format is considered and is converted to gray scale.
- Apply pixel management to the cover image, to avoid overflow and underflow
- Segmentation of cover image into 8*8 blocks and are transformed into DCT domain
- The number of bits *L* of each DCT coefficient of cover image to be replaced by the payload MSB bits using coherent bit length
- The steno image obtained in the DCT domain is converted into the spatial domain using IDCT.



Encoding Process

Decoding Steps: -

- The steno image is segmented into 8*8 blocks.
- The 8*8 blocks are transformed into frequency domain using DCT.
- The payload length *L* for each DCT coefficient is calculated similar to the procedure adapted in the embedding technique.
- Extract *L* bits from each DCT coefficients.
- The payload is constructed using *L* number of bits.



Decoding process

Creation of Public-Private Key Pairs and Public Key Certificates

The public key and the corresponding private key of each user is created locally by the user himself. An expire time is added to the generated public key. A thread is initiated to revoke the public key when it was going to expire at specific time. Generate an X.509 Certificate based on key pair. This Certificate (Cert) [3] is a self signed certificate that contains serial number, issuer public key, issuing time, expire time with digital signature. The certificate expire time will be less than expire time of the public key, means new certificate will be generated based on the old public key. Whenever the public key is revoked, the new certificate will be generated based on new public key.

These certificates are used to provide a session based authentication among the neighbors. More number of certificates are used in between two revocations of public keys. In the proposed scheme, issuing and revoking certificates are the only operations performed consciously by the users. All the other operations, including authentication, are performed automatically by the nodes, without direct user involvement.

Exchange of Public keys and Public key Certificates

After generating the public keys, each node offers its public key and expire time. This exchange process will be done in secure environment. The public keys are exchanged by easy handshaking process. After getting the neighbor public key, it will store in key repository (KR).

The node receives the public keys from every neighbor and sends reply messages. Every node send its certificate encrypted with destination public key only when it has destination public key and reply message of its own shared public key.

This certificate is encrypted with a symmetric key (SK) [4] generated for the current message. A digest will be encrypted with its own private key. The symmetric key will be encrypted with destination public key. We compose the message like this and send it to every neighbor who has the entry of public key in key repository and the reply message in reply repository. And expects reply message from its neighbor, which will be encrypted as sent message.

Construction and Exchange of Shared Key Repository and Trust Graph

After getting the neighbor certificates and reply message, each node will move to construct the shared key repository from the obtained public keys and expire times. At present moment, shared repository will have all the public keys of neighbors in key repository (KR).

Every node starts the process by constructing its shared key repository from its own key repository. Our main goal is, to wait until we get all public keys of nodes participated in the network. Till that, we wait in initial phase of the network.

Every node offers its own shard repository by filtering both of its primary keys to its neighbors. Means a separate key repository having the updated primary keys are sent to neighbors. In return, if the neighbors have other than these public keys, they will send their shared key repository. Each node receives its neighbor's shared key repository and updates its own shared key repository and informs about the updated information to other neighbors other than sender. Like this, each shared key repository will be updated with public keys of non neighbors. Along with this shared key repository, each node will construct a trust graph with the maintaining relationships as neighbors. We represent this graph as adjacency matrix and at each node, this graph will be constructed. Each node will send the shared key repository (SKR) and trust graph (TG) in encrypted form.

Revoking and Exchanging the Certificates and Public Keys

An expire time is assigned to each self signed certificate and a new certificate should be generated with the valid public key. This revoked certificate must be sent to all its neighbors and that message should be sent like a shared key repository, means should be attached with certificate. If any node sends a message with old certificate, then it should be authenticated [3]. To do this, every node has to save the previous certificate before the revocation. And immediately the node needs to send the new certificate to that neighbor. It is the responsibility of the node itself to send the updated certificates to all its neighbors. We follow the same process for public key revocation.

Revoking an Identity

In a PKI, there are a few well-known ways to revoke a public key certificate. From these, we can construct equivalent (or better) techniques in an IBC system.

The most prevalent mechanism for revoking a certificate is to create and publish a certificate revocation list. This list consists of revoked certificates together with the signature of a revocation authority, possibly the CA, to prove its authenticity. A revocation authority, possibly the PKG, can be created in an IBC system by designating an identity to it, e.g ”Revocation Authority”. The revocation authority can then create a list of identities to revoke and sign it with the private key corresponding to its identity. The advantage of IBC over a PKI is that identities (e.g. email or IP addresses) [3] are usually far smaller than certificates, resulting in a more efficient distribution of the revocation list.

Secondly, certificates usually have a validity period, which is defined as the period within two timestamps. Thus, the certificate expires, after which it is considered invalid. A new certificate must then be obtained. We can construct the same mechanism in an IBC system by requiring the validity period to be appended to the identity-string itself.

A third mechanism, perhaps less attractive, is to create a new set of system parameters and only give new keys to identities that are not revoked. This can be done when some threshold of revoked identities is reached, a time interval is exceeded or some other condition is met. This mechanism can thus be used in combination with a revocation list to avoid that the list grows indefinitely. The equivalent in a PKI is that the CA changes public key.

Threshold Cryptography

Practical cryptographic systems rely on the secrecy of keys to achieve any security. These keys may well be protected by encryption under other keys, but these encryption keys must also be protected. In the end, we must rely on that some keys are stored in a physically secure way.

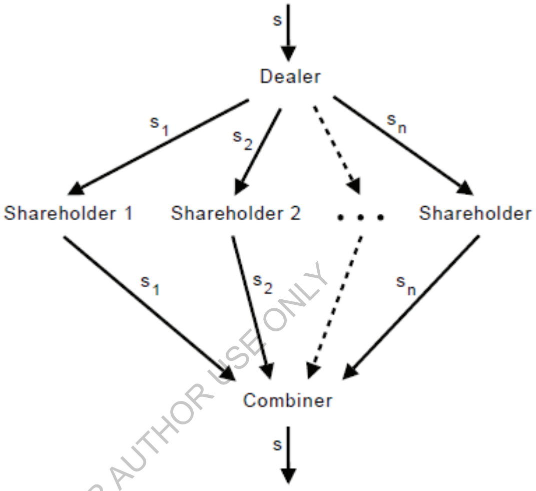
More risk is associated with the storage of some keys than others. In a PKI, the whole system is compromised if the private key of the CA is compromised. This also holds true for the master-key of the PKG in an IBC system. In a MANET, it is not always plausible to assume that any one node is physically secure. If a node holds the secret key corresponding to the public parameters of the system, an adversary may compromise the whole system by capturing one node. We are therefore particularly concerned that privileged keys are kept secret.

But privileged keys also need to be available. In an IBC system, the secret key corresponding to the system parameters is needed in order to generate keys for nodes. In a PKI, it is needed to generate certificates and revocation lists [5].

At first, the secrecy and availability requirements may seem contradictive: if we spread the key out on many locations to make it easily available, secrecy is degraded since the key is more prone to get compromised by an adversary. Threshold cryptography solves this problem by offering both secrecy and availability of information at the same time. Two important models for threshold cryptography are secret sharing and function sharing.

Secret Sharing

A threshold secret sharing scheme consists of a probabilistic algorithm, called the dealer, that takes as input a secret s, and outputs n shares s1, s2. . . sn. A threshold t, with t ∈ [1, n−1], is also defined. The idea is that any t shares reveal no information about the secret s, while any t + 1 share determines uniquely.



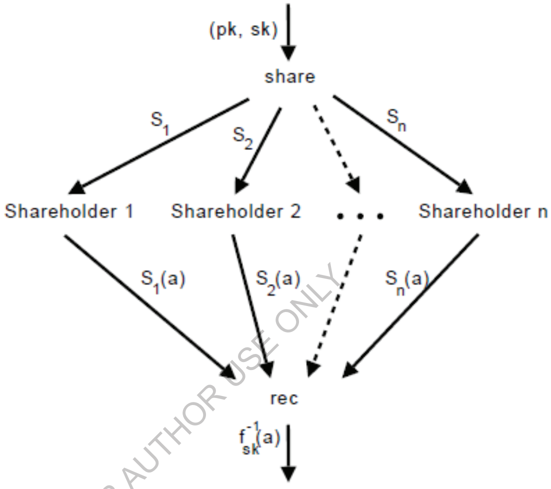
Secret Sharing

The dealer creates n shares, but this would be quite pointless if it held them for itself. So the dealer will distribute the shares to n shareholders, using a confidential and authenticated channel. The secret s is guaranteed to be kept confidential as long as no more than t shares are obtained by the adversary. When the secret s is needed, the combiner will collect at least t+1 shares, using a confidential and authenticated channel, and reconstruct s. The combiner may be one or more of the shareholders, or a separate entity.

Function Sharing

Secret sharing is a very powerful and versatile tool. However, if it is to be used to share a private key in a practical scenario, a problem arises: the combiner obtains the whole secret key when it is used in some computation. So if the adversary can capture the combiner, he may also compromise the private key. Thus [45], secret sharing is very useful for secure physical storage of a secret, but as soon as the secret is to be used, it is again very vulnerable to a compromise.

Some thought on this issue reveals that we do not really need to know the private key explicitly as long as we may use it in a calculation of some function. For example, the function could be to sign a public key certificate or generate a private key for a user as a PKG.



Function Sharing

It may seem a bit vague how we can use a secret without knowing it. But this is where the notion of secret sharing comes in: every shareholder has a share of the private key, but no one knows it. If we generalize this to functions, we could say that every shareholder has a share of the function, but no one knows the complete function. A common way to create shares of a function is to create a secret sharing of the input to the function, while the algorithm that is executed on the input is publicly known. In this scenario, the shareholders use their shares to do some local computations and then some entity combines the results of these computations to complete the function computation. Thus, by using function sharing [6], the combiner does not learn the secret s, but rather the output of a function where s is used.

It is probably possible to find cases where the algorithm executed in the shares of the function must be kept confidential, and the model that is presented next takes this into account.

However, we will only construct shares of functions by using secret sharing and keeping only the shares secret, while the operations on the shares are publicly known. Our on-going discussion on secret sharing is motivated by that we use secret sharing to construct function sharing.

Robustness

The availability requirement for a secret sharing scheme ensures that t + 1 share is sufficient to reconstruct the secret. But as shareholders may be corrupt, we cannot assume that any t + 1 shares obtained by the combiner are correct. Indeed, in Shamir's secret sharing scheme, if one of the t + 1 shares used by the combiner is incorrect, the secret cannot be reconstructed.

But worse, the error might not be detected and the output from the combiner is taken as the secret. Detecting an incorrect share is the topic of robustness.

A generic solution is to use Zero-knowledge protocols. These protocols can be used to prove that any communication or computation is done correctly, without revealing anything else (hence the name Zero-knowledge). However, the protocols are generally less attractive in practice because they are interactive and require much communication. Thus, robustness is most efficiently handled in an application-specific way.

Proactive secret Sharing

Secrecy ensures that the secret is kept confidential even though up to t shares are compromised, while availability ensures that the secret can be reconstructed if t + 1 valid share are obtained.

These requirements naturally lead to two goals for the adversary. He can try to obtain t + 1 shares to find the secret. But he can also destroy enough shares such that the secret cannot be reconstructed: destroying n − a t share leaves only t correct shares, which is insufficient to reconstruct the secret. Which one of the situations is the worst is hard to tell, but they are both clearly undesirable.

In general, it is impossible to reason about the probability for the adversary to succeed with any of these two goals. It clearly depends on the choice of n, t and the specific application where secret sharing is used. However, it is reasonable to say that the success probability for the adversary depends on how much time he has to his disposal, where more is generally better for him. Proactive secret sharing defends against a mobile adversary, where an adversary attacks one shareholder; either steals or corrupts his share, and moves on to the next [7]. The main idea is to periodically do share refreshing, where shareholders get new shares, leaving the old shares obsolete, while the secret remains unchanged. This forces the adversary to control enough shareholders within the same time frame (e.g. a week, day or hour), in order to succeed.

Removing Trust in the dealer

The dealer is trusted in two respects. Firstly, the sharing it creates should make the secret reconstructible. Secondly, it should keep the secret from leaking to the adversary.

Verifiable secret sharing a secret sharing scheme is verifiable if the shareholders may check that their shares can be used to construct an unambiguous secret, without revealing it. Multiple implementations exist, but all have in common that the dealer distributes some auxiliary information to the shareholders. Note that a malicious dealer may nonetheless share a different value than its input secrets.

Depending on the application, the exact value of the secret might not matter, as long as the sharings are consistent. Distributed key generation Suppose we want to share a private key of an asymmetric key pair, but we have no specific key in mind. Private Key needs to be random to be hard to guess, and some constraints on the key exist in order for it to be valid.

The idea of distributed key generation is to make each shareholder generate a share of the private key. This has the effect of removing the need for a dealer, and thus no entity knows the whole private key. It should however be possible to compute the corresponding public key without revealing the private key. Different protocols must be used when generating keys for different cryptographic systems.

Distributed Private / Public key Management

The Private Key Generator (PKG) plays an important role in an IBC system as it is trusted to store and use the master-key of the system. However, in a MANET, keeping a central PKG available and properly secured at all times is challenging, at best. We will consider how multiple nodes can share the authority of the PKG in a MANET. When the PKG authority is shared, we will refer to it as a Distributed Private Key Generator (DPKG) [8]. A DPKG consists of two protocols corresponding to the Setup and Extract algorithms, respectively. The first creates a secret sharing of the IBC system’s master key, while the latter is a function sharing of

Extract. A node having a share of the system's master-key will be referred to as a DPKG node. For example, every proposal includes a discussion on how a joining node obtains its private key corresponding to the system parameters. However, the issue of changing the set of DPKG nodes is not always addressed. Additionally, we argue that the meaning of security for a DPKG should be uniform. For these reasons, a generic characterization of a DPKG is useful. A major contribution in our following work is the definition of security for a Distributed Private Key Generator. As far as we know, this has not been addressed earlier. The definition may be used in any IBC system where threshold cryptography is applied to distribute the PKG authority.

During distributed Setup, we assume secure channels between all pairs of nodes, as constructed in the network formation phase. Recall that in an IBC system [8], the purpose of Setup is to generate system parameters. Note that most of the system parameters (e.g. hash functions, pairings, etc.) might be pre-established as universal standards because they are hard to generate, without compromising security. To generate the master-key in a distributed fashion, we can use a distributed key generation protocol.

The protocol run to generate system parameters will be denoted Ds. We say that ds completes successfully if it generates system parameters that have the same probability distribution as the parameters generated by Setup. After Ds is run, a MANET certificate may be created, which can be presented to potential joining nodes.

Results

The scenarios in which the tests were performed are very simple. The network is composed of only two nodes in the case of classical asymmetric cryptography, and three nodes in the case of IBC (the two communicating nodes, and the KGC). After the initialization phase takes place, we start measuring the time needed until the protocol is completed and the authentication succeeds.

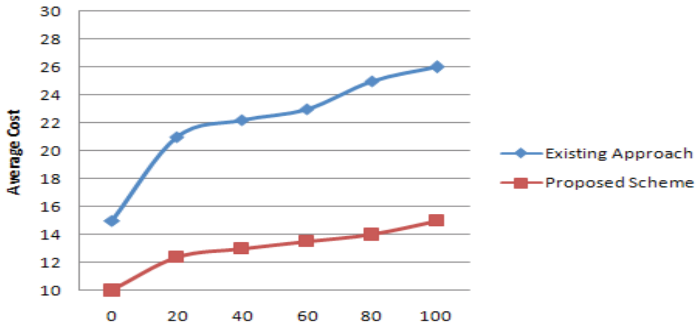
Pbits	**256**	**512**
Extraction Time	0.870s	2.903s
Encryption Time	5.710s	12.636s
Decryption Time	2.497s	5.830s
Plain Text Length	2KB	2KB
Cipher Text Length	4126KB	8224KB

Experimental Scenario

The trusted third party responsible for generating the private keys is called Key Generation Center (KGC). It computes the public parameters of the system that must be known by all the users in order to compute the public keys and to perform the cryptographic operations. Each of the users of the system receives these public parameters from the KGC and computes its public key and the public keys of the users it wants to communicate with. Then, it requests its private key from the KGC. The KGC computes the private key for each of the users starting from the public key of a user and using the private parameters that correspond to the public ones made available to all the nodes. Each node must receive the private key from the KGC on a secure channel, so that no eavesdropping is possible,

i) Cost Analysis

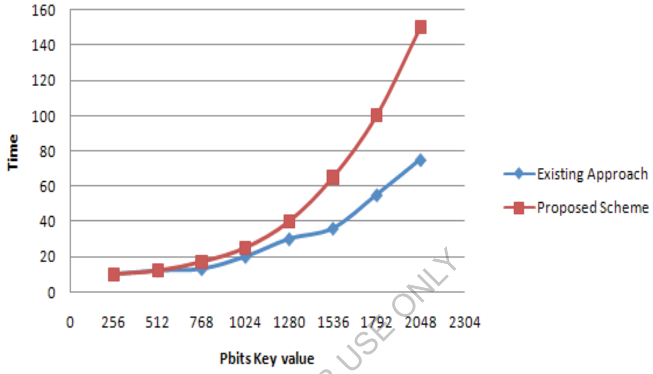
We perform simulations with 400 steps for 20 times and calculate the average cost of each time slot. Fig. 6.3 shows the cost comparison over the existing scheme when the first component in the state transition probability matrix changes from 0.85 to 0.98. With the increase of the transition probabilities (which is the probability that the node remains in its current state), the system becomes more secure and the proposed scheme always has lower cost than the existing scheme. The below figure shows the cost comparison when there are more nodes in the network. With the number of available nodes in the network increases from 6 to 30, the cost of all schemes becomes lower since there are more nodes that can be selected. The cost of the proposed scheme is shown to be lower than existing scheme in all circumstances.



Cost Comparison of availability of nodes

ii) Comparison Key Extract

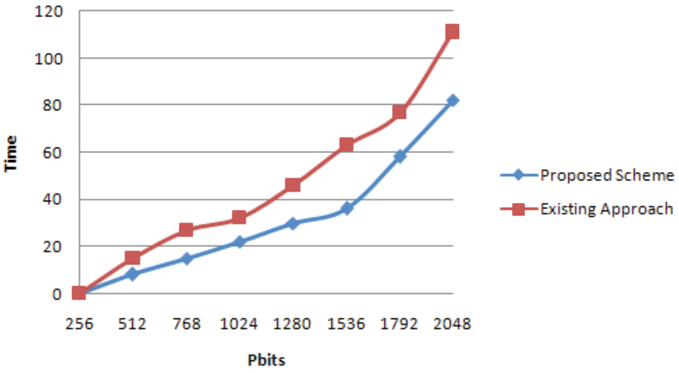
However, our test shows its performance is quite low. Even if the master key length is only 256 bits, the encryption/decryption speed is below 1KB/s, which cannot be acceptable in most cases. Moreover, the size of ciphertext is thousands times that of plain text. This conclusion is obvious, since for each bit of the message, the Encrypt algorithm returns two *P*-bit numbers. Therefore, considering both the time and space cost.



Key extraction from nodes

iii) Encryption Time

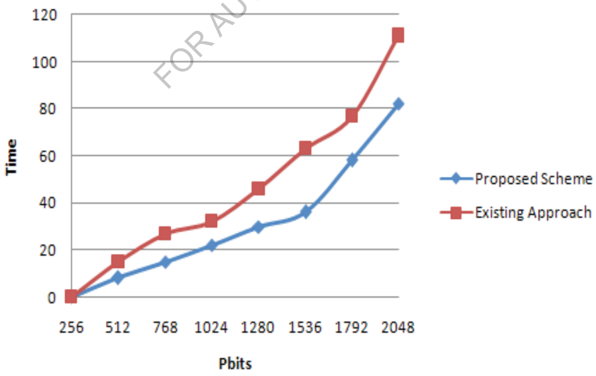
IBC require nodes to obtain authentic system parameters. But as soon as a node has obtained these, it may encrypt to all other nodes, and also check signatures generated by all other nodes — no certificates are required. The only requirement is that the node knows the identity of the other nodes. An identity may be any string, such as a name, email address or IP address. However, if the node wants to decrypt or sign a message, it will need the private key corresponding to its identity with respect to the system parameters. This private key is obtained from a so-called Private Key Generator (PKG). The PKG uses its knowledge of the master-key corresponding to the system parameters to generate the private key for any identity. The below figure, shows the proposed scheme is take less time to encrypt the message from the network.



Encryption Time from nodes

iv) Decryption Time

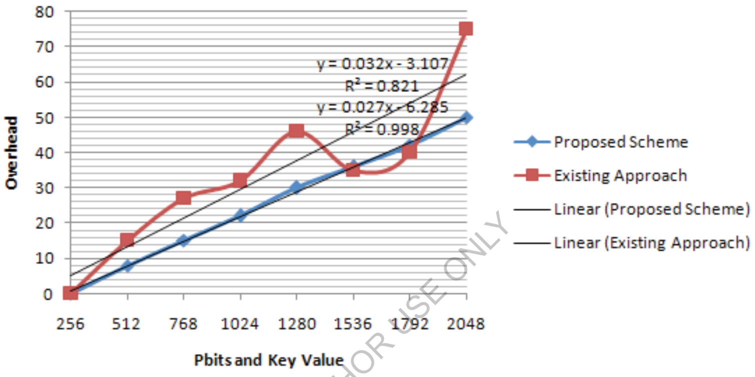
In an IBC, the PKG will know the private keys of all the users, so the PKG is more trusted in this sense. Furthermore, when the private key of a user is to be issued from the PKG, a confidential channel must be available. Otherwise, the private key may be compromised. This is not a problem in a PKI because only public keys are transmitted.



Decryption Time from nodes

v) Ciphertext Overhead

While the conventional PKI based key management approaches assume each node's public/private key pair is self-generated, and the public key is propagated in the network. In order to identify each node, the public key has to be signed by a trusted certificate authority (CA). The certificates are also required to spread in the network, so that each node can get other nodes' certificate. Propagating these public keys and certificates consumes a lot of network bandwidth, and also causes a large network/connection setup delay.



Cipher text Overhead for Probabilistic of nodes

We summarize our discussion with the main advantages and disadvantages of the sketched method for authenticating founder nodes. The most important advantage is that the authentication method is fully self-configuring; no pre established trust is required for the founder nodes. In addition, the nodes do not need any special physical characteristics (e.g. a GPS receiver, clock, etc.); everything may be implemented in software. On the negative side, manet nodes have limited, possibly varying, processing power. This may make it hard, maybe impossible in some cases, to find a function f that satisfies the requirements. But we believe that in order to achieve self-configuring authentication, we must consider alternatives to traditional authentication methods. However, it is interesting to note that the method we discussed here actually has similarities with a PKI. In a PKI, the CA creates a binding between a node and its public key. In our method, a processing unit creates the same binding.

Conclusion

When dealing with mobile ad-hoc networks (MANETs), one usually wants the network to work without the presence of any trusted third party. A natural way of achieving this property is by sharing among the nodes the role that such a third party would play. For this, an essential tool is the use of secret sharing techniques. However, the use of standard secret sharing techniques makes dynamism difficult to achieve. The special characteristics of a MANET result in frequent changes in the network topology. In order for routing to work in such a network, the routing protocol must take these characteristics into account. The OLSR routing protocol is specifically designed for MANETs, and we learnt how routing in MANETs can be done.

However, routing protocols for MANETs are vulnerable to a range of attacks, mainly because a MANET is based on wireless communication without any reliable infrastructure. Therefore, we examined different protocols that alleviate such attacks, by making them impossible or merely detecting them (i.e. intrusion detection systems). Through this study, we saw that a method for cryptographic key distribution and support for message authentication, e.g. from digital signatures, are needed. At the same time, the overhead induced by cryptographic mechanisms, especially on the bandwidth, must be very small for them to be applicable in a MANET.

All security mechanisms applied in networking more or less require the use of cryptography, which on the other hand implicates a strong demand for secure and efficient key management mechanism. In ad hoc networks the role of a dependable key management service is especially emphasized, given the constrained resources and possibly rapidly varying conditions in which the nodes operate. Traditional and centralized approaches cannot often be applied in the environments in which ad hoc networks operate, which force the use of distributed services that do not rely on single resources with respect to other nodes or communication paths.

In identity based cryptography, it is the Private Key Generator (PKG) that issues keys corresponding to identities. In order to support the self-configuring property of a MANET, the PKG must be online to issue keys to joining nodes. To protect the master-key of the PKG, but at the same time keep it available, we studied the theory of threshold cryptography, including secret sharing and function sharing. The PKG is involved in the Setup and Extract algorithms of an IBC system, so we focused on the distribution of these. But in addition, we discussed how signatures may be generated using a secret sharing of the master-key. This may be used to sign a message as the PKG authority, which is useful for instance when creating revocation lists. But we did not find any definition of security for distributed versions of Setup and Extract.

Any attack from the adversary may mainly have two undesirable effects. Firstly, the adversary may obtain important information. Secondly, he may cause denial of service by sending corrupted messages to the other nodes, or not send messages at all. Key management is a fundamental, challenging issue in securing MANETs. This work presents a secured ID-based key management scheme for MANETs which permits mobile nodes to derive their public keys directly from their known network identities and with some other common information. Most existing security mechanisms for MANETs thus far involve the heavy use of public key certificates. Our solution obviates the need of any inline Certification Authority (PKI) to share secret key. It also provides end-to-end authentication and enables mobile user to ensure the authenticity of user of peer node. The significant advantage of our solution is to avoid users to generate their own public keys and to then distribute these keys throughout the network. This scheme solved the security problem in the ad hoc network and is also suitable for application to other wired and wireless network.

More Books!
yes
I want morebooks!