International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 5; September 2017; Page No. 780-784

Routing protocols framework for secure communication in mobile wireless ad-hoc network

[1] Bhawna Sharma, [2] Sudesh Kumar
[1] Assistant Professor, GNG College, Yamunanagar, Haryana, India
[2] Associate Professor, GNK College, Yamunanagar, Haryana, India

Abstract
Wireless ad-hoc network is one of effective medium for mobile communication having facility for the sharing of resources and it introduces new services among the users. It is a group of wireless nodes that interact with each other without centralized control or fixed infrastructure. Routing protocols are vulnerable to routing attacks, data transfer is a major problem in ad-hoc network it lacks security and reliability of data. In this paper our focus is on security and data confidentiality during network communication. The proposed protocol framework for secure communication is completely self-configurable without any large network setup. It increases the performance of the system and provides security in the Mobile wireless Ad-hoc networks by using hybrid symmetric and initial trust between users for encryption and decryption of incoming and outgoing data packets.

Keywords: ad-hoc networks, relay node set, performance, wireless routing protocols, ad-hoc network security

1. Introduction
Wireless network is a type of network which does not require wires for establishing a connection between computer systems or network nodes for data transfer and this is based on the technology that uses the standard protocols for communication without physical cable connections. Mobile wireless Ad-hoc network is distributed network and it is a concept in computer communications which means that users wanting to communicate with each other from a temporary network without any form of centralized administration [1]. In which all activities of network are executed by the nodes, each nodes participating for communicate and forward packets for other nodes wirelessly [2]. For this purpose a, routing protocol is needed all routing functionality is merged into mobile nodes. A routing protocol is used to discover routes between nodes and it is use to minimize control traffic, such as periodic update messages, in which routers are used to form wireless networks [3]. This protocols in ad-hoc wireless networks can be classified into three broad categories, Proactive (or table-driven) protocols, Reactive (or on-demand) protocols, and Hybrid routing protocols, it is based on the routing information update mechanism; these Routing protocols are vulnerable to routing attacks [4]. There are various routing attacks in this network using Impersonation, Modification, Fabrication, Replay, and Denial of Service (DoS), any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network [5].
There is two types of communication: direct and indirect; in direct communication, nodes that are in radio range of one another can interact with each other directly while in indirect communication, nodes interact with each other with the help of intermediate nodes in order to route their packets. Wireless interface is used through which each node communicates.

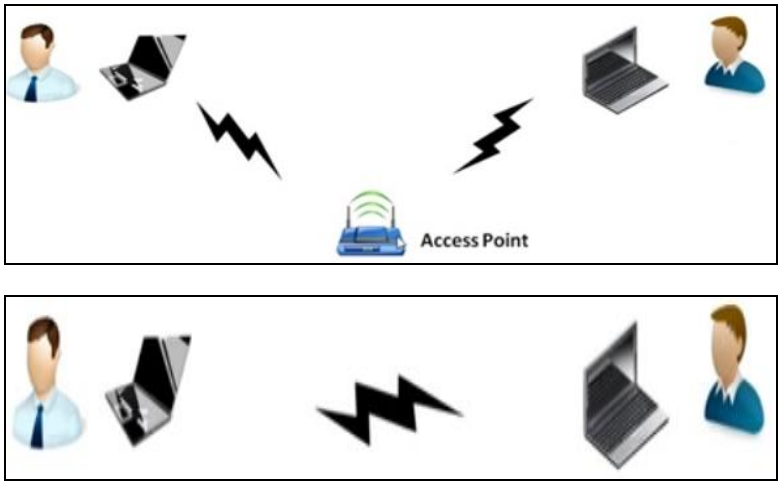

Fig 1: Direct or Indirect Connection.

Wireless ad hoc network is mutihop network having self-configured, self-optimized data network because it separate from the other external networks. Therefore, security issues are the main challenges for the wireless ad hoc network communication. Our objective is to integrate the services and devices in such way that they do a secure communication in the wireless ad hoc environment and in this project first we will do clustering with the help of K-Means Algorithm and other efficient methods, if we have a new node present in the network then we do new node addition with the help of SET-IBS protocol mechanism [9, 10, 11].

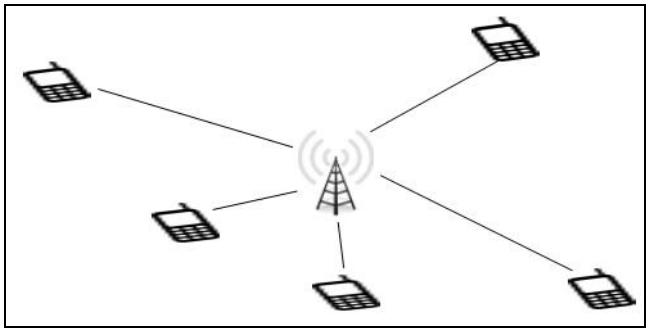

Fig 2: Mobile Ad-hoc Network.

Proposed secure procedure is designed for unplanned wireless ad hoc network which uses a hybrid symmetric and asymmetric scheme. Symmetric and asymmetric keys are used for security management. A various security scheme provides a completely independent Protocol and it will help to share secured services without any infrastructure by creating a new network. The proposed protocol framework for secure communication is completely self-configurable without any large network setup and Inter network communication with the help of ECC (cryptography) and k-means algorithm for clustering.

2. K-means algorithm for clustering in Mobile Ad hoc Network

Routing in a network is the process of selecting paths to send network traffic. Routing can take place either in a flat structure or in a hierarchical structure. This approach consists of dividing the network into groups called clusters. This results in a network with hierarchical structure. Different routing schemes are use between clusters (inter-cluster) and within clusters (intra- cluster). Hierarchical routing is a solution for handling scalability in a network.

K-means clustering technique is one of the significant clustering algorithms that can solve many routing problems in MANETs [12]. Due to easy implementation and fast convergence, K-means clustering is an applicable clustering method specifically in mobile ad hoc networks. In contrast, there are some limitations like inadequate distribution of nodes in clusters, fixed cluster head and cluster members. The first step of K-means is to select as initial cluster centers K. The algorithm follows a simple way to sort out a specific data group through a distinct number of clusters (assume k clusters). The main idea is to determine k centroids, each centroids belongs to one cluster. The cluster head plays the role of coordinator within its substructure. Each CH acts as a temporary base station within its cluster and communicates with other CHs [13, 14]. A cluster is there-fore composed of a cluster head, gateways and members node.

1. Cluster Head (CH):-it is the coordinator of the cluster.
2. Gateway: - is a common node between two or more clusters.
3. Member Node (Ordinary nodes):-is a node that is neither a CH nor gateway node. Each node belongs exclusively to a cluster independently of its neighbors that might reside in a different cluster.

3. Elliptical curve cryptography (ECC) in mobile ad-hoc network

Cryptography is a recent branch of cryptography based on the arithmetic of elliptic curves and the elliptic curve Discrete Logarithm Problem (ECDLP).The main objective of cryptography is to protect our data by using different authentication schemes. Two main terms that is used for the cryptography technique are Encryption and Decryption. Encryption technique is used to send confidential data over communication. Decryption is the reverse process of encryption. It is technique to convert the encrypted data to its original data that is now readable [15]. ECC is emerging as an attractive public-key cryptosystem for mobile/wireless environments. ECC is used because of its small key size. Cryptography is an electronic technique. It is used to protect valuable data while communicating. A secret key management scheme can be used to encode and decode the incoming and outgoing data respectively in this network communication and with help of it the data in the network is protected from external attackers.

The [16] mathematical operations of ECC is defined over the elliptic curve $y^2 = x^3 + ax + b$, a and b are elements of a finite field with elements, where p is a prime number which is selected as larger than 3.The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field and such that x and y satisfy the relation given by the equation $y^2 = x^3 + ax + b$ defining the curve, plus an extra point that is said to be at infinity.

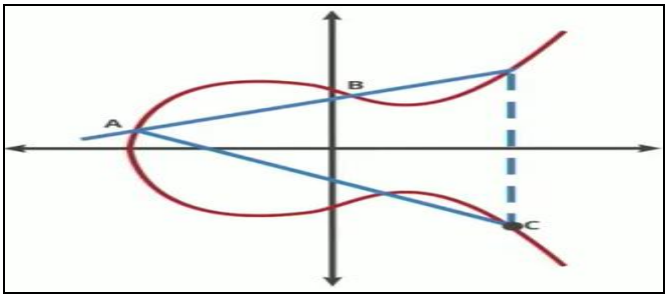

Fig 3: Mathematical operations of ECC

4. Related Work

Zhiguo Wan [17] shows the demand of the secure routing protocol for the mobile ad hoc network as the privacy of certain networks is fundamental requirement.

Marc Danzeisen [18] implemented a cellular framework for successful spontaneous network establishment. This offers a dashboard-like tool, which can, with the help of a cellular network, ease the formation of spontaneous networks among

heterogeneous nodes. Furthermore the provided implementation is able to secure the acquired communication links in the spontaneous network and therefore protect the exchanged information against possible abuse.

Juhani latvakoski [19] Present a communication Architecture for Spontaneous Systems in this papers author take communication types as peer to peer, there no specific security scheme is going to define by the author. When the ad hoc nodes which is mobile it must have a several security schemes for the secure communication between the nodes, and in implementation of the cellular mobile network is shown, it may be used in the ad hoc network.

Raquel Lacuesta uses the hybrid symmetric or symmetric schemes which include the initial data exchange on basic of user's reliance. In this paper reliance is based upon the first visual contact. The proposed system having the autonomous protocol which helps in secure communication in network node and also it do not need any large infrastructure [20].

Zygmunt J. introduces a secure and self-automated fault tolerant communication network as the design of the network change. Here paper proposed a protocol to evaluate the malicious disruption of the data in the message transmission they called it as the secure transmission protocol and secure single path protocol [21] but these protocols are run solely on the trust basic of the network and security associations. As the result of this the network may having the security issues as any malicious node is present in the network.

As wireless ad hoc nodes having mobility it causes frequent changes in the topology of a network. If certain node moves out of radio range of network then link is broken such types of networks are very useful for the defense purposes [22], but when the link is broken down then reorganized node data must be updated on the base station of wireless ad hoc network for the security concern.

Chi Zhang design a identity based cryptosystem which delivers necessary security requirements to the network Ad hoc network is more significant way that other network cannot able to attack on the network and the challenging issues are discuss in [23], As the ad hoc network having the self-structured mechanism and key management is one of the important part of it and for the encryption algorithm a public key management technique is introduced in ad hoc network Ad hoc network forms the cluster on the basic of their geological location or energy constraints we may take another parameter for it. In [24] proposed the two protocols for the secure data transmission in the cluster based ad hoc network.

As the data communication in the ad hoc network is done in a secure way then for the encryption and decryption researchers proposed a safe and sound cluster base key management technique [25] which uses distributed authorities and also proposed a robust re clustering algorithm.

5. Proposed Optimization Scheme

Our Protocol Framework can be applicable to wireless ad hoc network, standalone network where all the service of the network are self-configured by the network users and nodes for the secure transmission of the data, Here we considered (n) nodes in the network which is nothing but the network user which are going to share the network resources and take part in the network communication. We used k-means algorithm for initial cluster formation and on the basic of their geological location we elect the base station in the on network we have several group of wireless ad hoc network and which are connected with the direct link between the respective base stations. We have a tendency to propose two secure and economical knowledge transmission (SET) protocols for secure communication referred to as SET-IBS and SET-IBOOS, by victimization the identity-based digital signature (IBS) theme and the identity-based online/offline digital signature (IBOOS) theme, severally. In clustering module we are going to create the node by using the k-means cluttering algorithm, we have base station in ad hoc network for centralized control, which gives various services to the cluster heads in the network. Cluster head is form in the network on the basic of their energy level or geological position. Dynamic cluster head is elected on the basic of their energy levels. If cluster head lost energy then it will switch to another cluster head which having high amount of energy in this scenario we may consider take other parameter for the cluster formation in network. We proposed an efficient technique, which is able to do clustering of network with respective to their correlation; we used Data Density Correlation Degree Clustering Method [26] in an efficient way to do the clustering in this protocol. We do the cluster head election means we have the cluster head for each cluster and in the network there is one or more clusters, here cluster head is equal to the number of clusters present in the network.

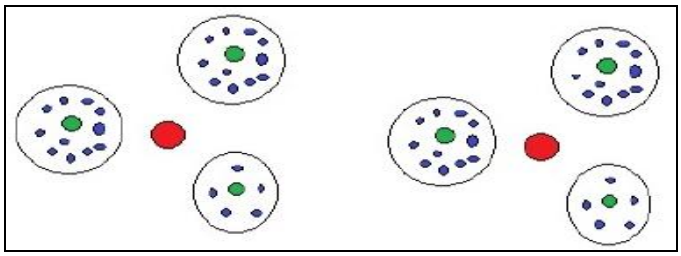

Fig 4: Flow Diagram of Transmission in MANET

Red Point showing Base Station
Green Point showing CH (Cluster head)
Blue Point showing Cluster Node

Several types of communication (Figure 4) in the ad hoc network that are, one base station to another base station, base station to cluster head and cluster head to cluster node. We used cryptosystem for the encryption and decryption of data, which is based upon the ECC to fulfill the purpose of the secure communication in the network. In the proposed system consist of three system module which is shown in figure 3, first module in for the creation of clusters for the group communication; second module is for the addition of the new node in the network and the third module is for the inter network communication. The basic working Steps in Secure Wireless Ad Hoc network are:

1. Joining procedure
2. Accessing the services
3. Constructing trust chain

Step 1

When a device wants to join a Wireless ad hoc network it has to start the process by sending a Discovery request packet (say

packet A), which contains the Logical Identity of the user in order to know destinations the sender device. The receivers will reply include the Discovery reply packet (say packet B) and it includes Identity, their IP address and network mask in the reply packet.

Step 2
The Authentication request packet (say packet C) is used for the new device authentication. The authentication reply packet (say packet D) confirms that the proposed IP and the email are unique in the network, so the new device is formally authenticated.

Step 3
The IP and e-mail checking packet (say packet E) is used by the authenticator device to verify that no one in given network has the same email or IP address as the one proposed by the new device.

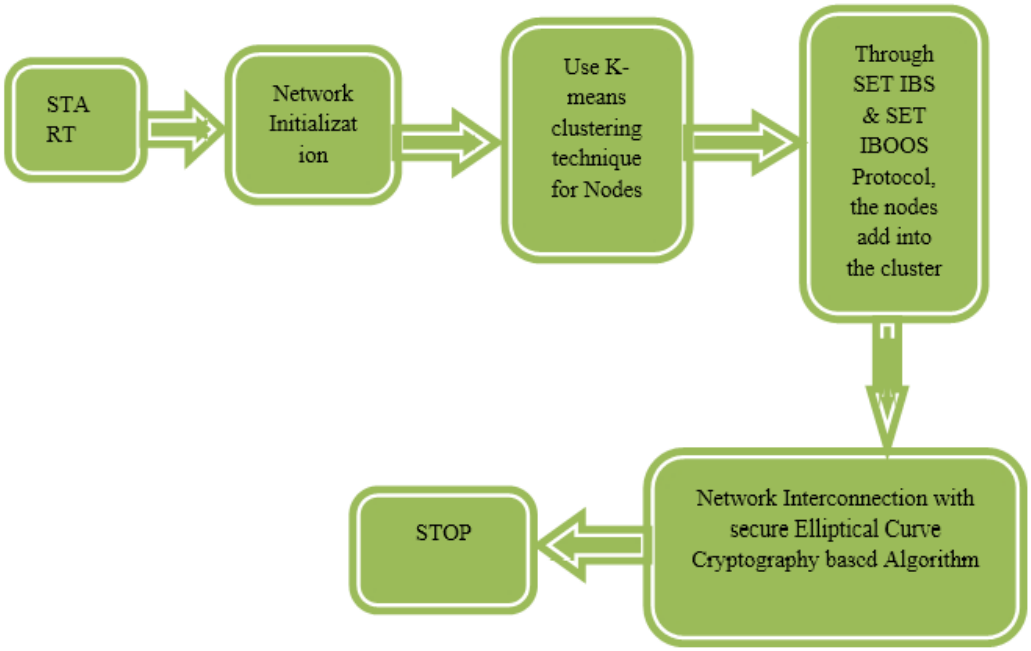

Fig 5: Framework Structure.

6. Conclusion
This paper proposes a secure data communication protocol for the wireless ad hoc network that allows creating and managing the wireless ad hoc network in a secure way. This protocol can be used in defense purposes and many other areas where data security and privacy on a top priority. We used various algorithms and techniques to form clusters in the network and for achieving centralized control over the network we elected the based station of a network and cluster head of each cluster in the network. We introduced protocol in the user responsive background for the easy access. The security schemes used in this protocol ensures the secure communication over the wireless ad hoc network.

7. References

1. Tonny Larsoon, Nicklas Hedman. Routing protocols in wirless ad-hoc network, a simulation study, Lulea University of technology, 1998. ISSN- 1402-1617.
2. Harjinder Kaur, Sukhjit Singh. Wormhole Attack Detection and Prevention in MANET Using Bait, IJESC, 2017.
3. Monika Shivhare1, Prof. Praveen Kumar Gautam. Prevention of Black Hole attack in MANET Using Indexing Algorithm, IJESC, 2017.
4. Seryvuth Tan, Keecheon Kim. Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs IEEE, 2013.
5. Li Wenjia, Joshi Anupam. Security Issues in Mobile Ad hoc networks (A Survey), The 17th White House Papers Graduate Research In Informatics at Sussex, 2004.
6. Panagiotis Papadimitratos. Member, IEEE, and Zygmunt J. Haas, Senior Member, IEEE, Secure Data Communication in Mobile Ad Hoc Networks IEEE Journal On Selected Areas In Communications, 2006.
7. Lidong Zhou, Zygmunt J. Haas Cornell University, Securing Ad Hoc Networks, IEEE transactions on Network, 1999.
8. Zhiguo Wan, Kui Ren, Ming GU. USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks, IEEE transactions on Wireless Communications, 2012.
9. Huang Lu. Student Member, IEEE, Jie Li, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE, Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks IEEE transaction on Parallel and Distributed systems, 2012.
10. Tselikis C, Douligeris C, Mitropoulos S, Komninos N. Consistent Re-clustering in Mobile Ad Hoc Networks IEEE, 2008.
11. Lung-Chung Li, Ru-Sheng Liu. Securing Cluster-Based

Ad Hoc Networks with Distributed Authorities. IEEE transactions on Wireless Communications, 2010.
12. Zohu L, Haas Z. Securing Ad Aoc Networks" IEEE-Network Magazine, 2000.
13. Anupama M, Sathyanarayana B. Survey of Cluster Based Routing Protocols in Mobile Ad hoc Networks. International Journal of Computer Theory and Engineering, 2011.
14. Gupta N, Shrivastava M, Singh A. Cluster Based on Demand Routing Protocol for Mobile Ad Hoc Network, IJERT, 2012.
15. Thambiraja E, Dr. Umarani R, Ramesh G. A Survey of the Elliptic Curve Integrated Encryption Scheme. International Journal of Advanced Research in Computer Science and Software Engineering, 2012.
16. Certicom. Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, 2000.
17. Juhani Latvakoski, Danielpa Kkala, Pekka Paakkonen. Vtt Technical Research Finland Kaitovayla, A Communication Architecture for Spontaneous Systems. IEEE Wireless Communications, 2004.
18. Winiker S, Danzeisen M, Rodellar D, Braun T. Implementation of Cellular Framework for Spontaneous Network Establishment, Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), 2005.
19. Marc Danzeisen, Torsten Braun, Simon Winiker, Daniel Rodellar. Implementation of a cellular framework for Spontaneous Network Establishment. IEEE Communications Society / WCNC, 2005.
20. Panagiotis Papadimitratos. Member, IEEE, and Zygmunt J. Haas, Senior Member, IEEE, Secure Data Communication in Mobile Ad Hoc Networks IEEE Journal On Selected Areas In Communications, 2006.
21. Lidong Zhou, Zygmunt J. Haas Cornell University, Securing Ad Hoc Networks IEEE transactions on Network, 1999.
22. Zhiguo Wan, Kui Ren, Ming GU. USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks IEEE transactions on Wireless Communications, 2012.
23. Srdjan Capkun. Student Member, IEEE, Levente Buttya´ n, Student Member, IEEE, and Jean-Pierre Hubaux, Senior Member, IEEE, Self-Organized Public-Key Management for Mobile Ad Hoc Networks IEEE transactions on mobile Computing, 2003.
24. Selva Reegan A, Baburaj E. Key Management Schemes in Wireless Sensor Networks: A Survey International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013] 2013.
25. Hemalatha Jai Kumari E, Kannammal. A Energy analysis of Public-Key Cryptography for Wireless Sensor network ICCCNT, 2012.
26. Fei Yuan, Yiju Zhan, Yonghua Wang. Data Density Correlation Degree Clustering Method for Data Aggregation in WSN IEEE SensoSrs Journal. 2014.