Trust based Clustering and Secure Authentication for Multicast in AD-Hoc

M. Ellcy Priana
Assistant Professor
Sir Issac Netwon College of Engineering and Technology
Nagapattinam, India

ABSTRACT
Ad-hoc network is a dynamic wireless network, composed of mobile nodes without the aid of centralized administration, where nodes have limited transmission range. Security is challenging issue due to the mobility of nodes can lead to dynamic topology, intermediate nodes act as a router can forward packets. Therefore authentication the source and forwarding packets with cryptographic mechanism and valid MACs is inappropriate because the data with encrypted key can send in same path can be modified by the attacker node. This paper presents a clustering mechanism with multi-hop communication and the source authentication is also done. The agent node is developed to verify the key with encrypted data is modified or not. The key management is done by the agent node. This ensure the source forwarding data is modified can be send using different path using dynamic selection of paths. The multicast protocol with hierarchical routing will increase the scalability.

Index Terms
Secure authentication, multicast communication, key managament.

1. INTRODUCTION
In recent years the ad-hoc network has tremendous applications like commercial and military potential such as battlefield communication, embedded sensor devices and for the research areas like asset tracking, digital battlefield situational awareness. In ad-hoc network the protocol plays a vital role. The multi-hop communication is important for providing large set of nodes for increasing scalability. In particular the provided network services need to achieve the security goals. The first one is confidentiality for encrypting the data receives from the source. The second one is source authentication with agent node.

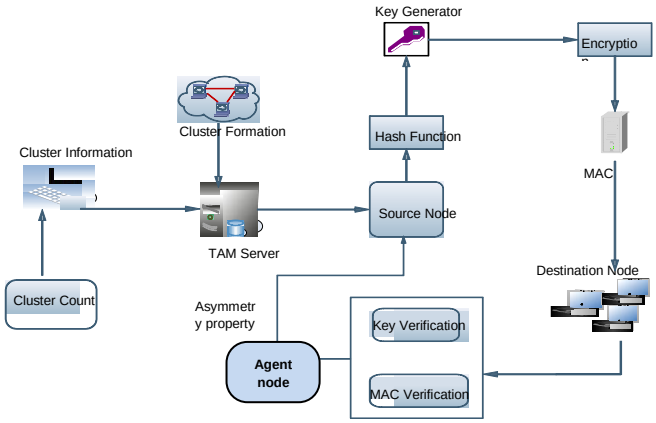
Multicasting plays a role in ad-hoc network application thus it will improve the performance of network. There are some issues regarding multicast such as robustness, efficiency and resource managament. The ad-hoc is a self-organizing network form an arbitrary topology. Indeed, we take advantage of existence of three different paths which increase the security of data.

Security is major factor for the network has to achieve security requirement such as confidentiality, authentication, integrity, availability.

The main goal of key management in a network between source to destination is to encrypt\decrypt the message using cryptographic technique. If there is an absence of key management leads to an attacks. Therefore key management is a primary concept for the communication in a secure way. In other point, the node act as a source can send message to receiver node are not directly connected the intermediate nodes who act as a router. The source and receiver node also act as an intermediate node. Thus in this multi-hop the attacker node can modify data, update data in the absence of secure protocol. In this paper, proposed a key management using one way hash function such as MD5, SHA-1, etc., The source generates the one time keys using hash. The MD5 can used as a digital signature. The On-demand routing protocol can be based on request the message will be send to a particular destination or receiver.

Cluster based routing protocol is a hierarchical protocol, which can be used to improve scalability. The cluster-head and the member nodes also there in each cluster. The source send data to destination floods packets after receiving the cluster-head analyses the destination .is in their cluster or not. The request is again send to the same cluster means it reject the packet if the address is seen again. The destination receives the data it can reply back with the route that has been recorded. The agent node will monitor the attacker node who is sending request the cluster is not acceptable because the cluster head who agent node will find the whether is the node is attacker or legitimate node.

2. ARCHITECTURE OF THE PROPOSED SYSTEM

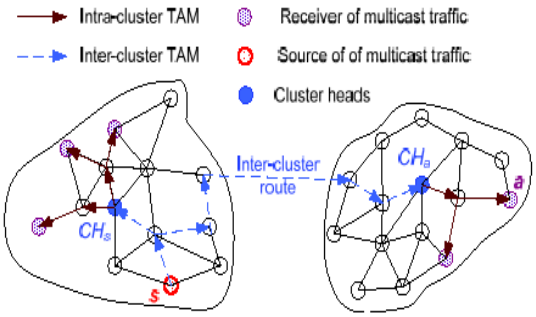


2.1 Cluster Based Routing Protocol
The cluster with a multi-hop can have nodes as members and have the cluster head for each cluster. The cluster information is stored as who is the cluster head and the cluster head changes due to the security aspects. The least cluster change should be done. Thus the neighbor maintains a adjacent table for information stored about cluster. When the source send to destination who is requesting the packet the cluster head checks the cluster is in the cluster or not. If yes, the cluster head address is recorded for discarding a packet is already seen. The random way of path selection is done. If there is an node which is to be broken it can check whether the next hop is available or not. This cluster protocol can be used to provide security in a trusted way and increases scalability.

2.2 Existing System

In the recent years, the ad-hoc is challenging in many areas like scalability, security and bandwidth constraint. The self organizing is required in ad-hoc for neighbor discovery, topology organization. The tiered authentication for multicast is done in multi-hop fashion, the clustering formation improves an scaling to large area of network. The protocol using forms a clustering mechanism without the use of different path to send packets to destination.

The authentication using a cryptographic technique and MAC code provide security [1]. There is a absence of different path selection for key with data that leads to attacker more easy to hack and modify data. The clustering forms a cluster head and other nodes as members. The cluster gateway proactive protocol is used to set to large network. The network with secure manner, is based on the secure way of mechanism. The cluster formation used in this cluster gateway routing protocol is given in diagram as



2.3 Proposed System

In proposed work, secure clustering and source authentication is done. The data modification by the attacker is verified by the agent node. It provides the confidentiality based on the encrypted key generated by the source. It can be passed through the source node to all member nodes using same path. The cluster based routing algorithm can be followed. The cluster is formed in a multi-hop mechanism, the cluster information is stored. Each node can have cluster information such as cluster name, header name, nodes name. The nodes with node name, with header node can be maintained and the topology can be created. In a cluster the new node enters it can be verified only by the agent node. If a node terminates, then it can of malicious node it can made a link to neighbor node. The agent node which is used to monitor the data with encrypted key is modified by the attacker or malicious node. Thus the trusted clustering and the multicast protocol which provides security.

3. CONCLUSION

In this paper, proposed work the secure clustering with the key management is done for security in ad-hoc network. The cluster based routing mechanism with key management for large network will reduce attacker threat to the network.The agent node will monitor the nodes which provide security and scalability is improved by large scale of network. Thus our scheme should provide a secure and scalable network.

4. REFERENCE

[1] ”TAM: A Tiered Authentication of Multicast Protocol for Ad-hoc Networks,” Mohamed Younis, Osama Farrag and Bryan Althouse, In Proceedings of IEEE Transaction on Network and Service Management, Vol.9, No.1,March 2012.

[2] ”Secure clustering and symmetric key establishment in heterogenous wireless sensor networks,” R. Azarderskhsh and A. Reyhani-Masoleh, In Proceedings of IEEE Transaction on EURASIP J. Wireless Commun. Netw., Vol.2011, article ID 893592, 2011.

[3] ” Trust management in mobile ad hoc networks using a scalable maturity-based model,” P. B. Velloso, et al., In Proceedings of IEEE Transaction on Network Services Management, vol. 7, no. 3, Sep. 2010.

[4] ”A hierarchical identity based key management scheme in tactical mobile ad-hoc networks,” F. R. Yu, H. Tang, P. Mason, and F. Wang, In Proceedings of IEEE Transaction on Network Services Management vol. 7, no. 4, pp. 258–267,Dec. 2010.

[5] .“Group-based source authentication protocol for VANETs,” Y. Lu, B. Zhou, F. Jia, and M. Gerla, In Proceedings of IEEE GLOBECOM Workshop Heterogeneous, Multi-hop Wireless Mobile Networks, 2010.

[6] “Overlapping multihop clustering for wireless sensor networks,” M. Youssef, A. Youssef, and M. Younis, In Proceedings of IEEE Transaction on parallel Distribution System., vol. 20, no. 12, pp. 1844–1856, Dec. 2009.

[7] “A survey of multicast routing protocols for mobile ad-hoc networks,” L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, IEEE Commun. Surveys & Tutorials, vol. 11, no. 1, pp. 78–91, first quarter 2009.

[8] “Location-aware combinatorial key management scheme for clustered sensor networks,” M. Younis, K. Ghumman, and M. Eltoweissy, In Proceedings of IEEE Transaction on Parallel Distribution System., vol. 17, no. 18, pp. 865–882, Aug. 2006.

[9] “An authentication service based on trust and clustering in wireless ad hoc networks: description and security evaluation,” E. C. H. Ngai and M. R. Lyu, in Proceedings of IEEE International Conf. Sensor Networks, Ubiquitous, Trustworthy Computing , 2006.

[10] “A survey of clustering schemes for mobile ad hoc networks,” J. Y. Yu and P. H. J. Chong, ,” IEEE Commun. Surveys & Tutorials, vol. 1, no. 1, pp. 31–48, 2005.