E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

A STUDY ON SECURITY SCHEMES OF CLUSTERING IN MANET

Vishnu Priya.S[1],Rani.V.G MCA,M.Phil,(Ph.D)[2]
[1]M.phil Scholar comp sci deptt, [2]Associate Professor comp sci deptt.
Sri Ramakrishna College of arts and science for women
Coimbatore, Tamil Nadu,India
vishnupriya.santhanam@gmail.com

Abstract:
Cluster structure is the solution in the large scale MANET to enhance the network scalability. Current technologies and security advances have made networks systems and applications very popular and broadly used. The enveloping and practical aspects of wireless Mobile Ad Hoc Networks (MANET) made them very popular as well this created the need for securing MANET's to provide users with authentic communications, safe, and robust information exchange and efficient security mechanisms .However, many of the security Solutions devised for regular networks are not as efficient or as effective on MANET's. In this paper various security scheme of clustering have been introduced.

Keywords-*Security; MANET; Clustering.*

1. INTRODUCTION

In recent performance advancements in computer and wireless communications technologies, highly developed mobile wireless computing is expected to see increasingly widespread use and application, much of which will engage the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes.

1. 1 Challenges in MANET

The technology of Mobile Ad hoc Networking is somewhat synonymous with Mobile Packet Radio Networking (a term coined via during early military research in the 70's and 80's), Mobile Mesh Networking (a term that appeared in an article in The Economist regarding the structure of future military networks) and Mobile, Multihop, Wireless Networking (perhaps the most accurate term although a bit cumbersome). There is present and future need for dynamic ad hoc networking technology.

The emerging field of mobile and nomadic computing, with its current importance on mobile IP operation, should progressively broaden and require highly-adaptive mobile networking technology to effectively manage multihop, adhoc network clusters which can operate originally or, more than likely, be attached at some point(s) to the permanent Internet. MANET can be established extremely flexibly without any fixed base station in battlefields, military applications, and other urgent situation and disaster situation. Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange.

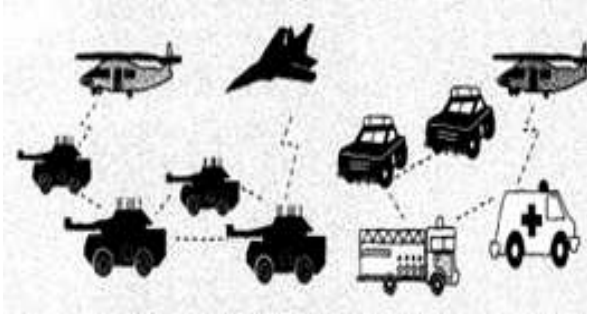

Figure 1 Application of MANETs

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

In addition, mesh-based mobile networks can be operated as robust, cheap alternatives or enhancements to cell-based mobile network infrastructures. There are also existing and upcoming military networking needs for robust, IP-compliant data services within mobile wireless communication networks many of these networks consist of highly-dynamic autonomous topology segments. [9]

1.2 Characteristics of MANETs

MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily.

The nodes may be located in or on airplanes, ships, trucks, cars, maybe even on people or very small devices, and there may be several hosts per router. A MANET is a free system of mobile nodes.
MANETs have some salient characteristics:

1.2.1 Dynamic topologies

Nodes are free to move impartially, thus, the network topology--which is usually multi hop-may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

1.2.2 Bandwidth-constrained, variable capacity links

Wireless links will continue to have significantly lower capacity than their hardwired counterparts. Besides, the realized throughput of wireless communication after accounting for the effects of multiple access, diminishing, noise, and interference conditions and so on is often much less than a radio's maximum transmission rate. One consequence of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, which is aggregate application demand will likely approach or exceeds network capacity frequently.

1.2.3 Energy-constrained operation

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most vital system design criteria for optimization may be energy conservation.

1.2.4 Limited physical security

Mobile wireless networks are generally more prone to physical security threats than are rigid- cable nets. The enlarged option of eavesdrop, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are frequently applied within wireless networks to reduce security threats.
The aim of this paper is to provide security for clustering in MANET. The results presented in this paper will help us to design to select appropriate clustering security techniques for MANET.

This paper is organized into six sections. Section-2 Security Objectives Section-3 Attacks On ADHOC Network Section-4 literature survey Section-5 Table Section-6 conclusion

2. Security objectives

The preliminary security goals can be considered as an extension of the objectives for traditional Networks. Two mnemonics, ‘CIA’ (Confidentiality, Integrity, Availability) and ‘Triple A’ (Authentication, Authorization, Accounting) are generally used as the criteria for a secure network.

These attributes must be satisfied, as well as some other factors like privacy, physical security etc. must be considered due to the pervasive nature of MANET.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

2.1 Confidentiality

The information must not reach others, who are not entitled to receive the information. Not only data, routing information must also remain secure.

2.2 Integrity

One shouldn't be able to modify the data during transit. Both malicious attacks and benign failure, such as radio propagation impairment could cause information corruption.

2.3 Availability

The network can still operate when faced with a DoS attack. These types of attacks can be launched at any layer of the network causing physical jamming, disconnection, and malfunction of key management service and routing protocol.

2.4 Authentication

The receiver should be able to identify the sender correctly. No other person can masquerade as the sender.

2.5 Non-repudiation

The sender can't falsely deny later that he has sent a message. This is useful for detection and isolation of compromised nodes.

2.6 Access control

Information is being handled by authorized nodes.

2.7 Authorization

Rules and regulations that define restriction of responsibilities of network as well as individual nodes.

3. ATTACKS ON MANET

There are diverse types of attacks on Adhoc network which are describing following:

3.1 Location Disclosure

Location disclosure is an attack that targets the privacy requirements of an ad hoc network. During the use of traffic analysis techniques or with simpler probing and monitoring approaches, an attacker is able to determine the location of a node, or even the structure of the total network.

3.2 Black Hole

In a black hole attack a malicious node injects false route replies to the route requests it receives, advertise itself as having the shortest path to a destination. These fake replies can be made-up to divert network traffic through the malicious node for eavesdropping, or merely to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

3.3 Replay

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the originality of routes, but can also be used to undermine badly designed security solutions.

3.4 Wormhole

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network .One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunnelled traffic back into the network. The connectivity of the nodes which have established routes over the wormhole link is completely under the control of the two colluding attackers. The solutions to the wormhole attack are packet leashes.

3.5 Blackmail

This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may construct such reporting messages and try to isolate legitimate nodes on or after the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generate (11)

4. STUDY OF RELATED WORKS

According to Avinash Jethi et al., [1] this paper presents wireless ad hoc network which communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized method. The principle behind ad hoc networking is multi-hop relay, which means that the messages are transmitted by the other nodes if the target node is not directly available. For communications with the nodes which are not within the radio range of nodes to the route must be taken from the intermediate nodes to reach the destination. These intermediate nodes act as router which receives the data coming from the source and forwards the data to destination. This state is of potential security concern as there can be attack possible by the intermediate node like Man in Middle Attack. Therefore an authentication procedure is be used for authenticating the mobile nodes to each other and proper encryption decryption mechanisms is also employed. Also middle nodes can act as malicious nodes which must be removed or alternate route should be found which does not include nodes already used in previous route.

According to Bechler.M et al., [2] they propose and evaluate a security concept based on a distributed certification facility. A network is separated into clusters by means of one special head node each. These cluster head nodes carry out administrative functions and hold shares of a network key used for certification. New nodes start to contribute in the network as guests; they can only become full members with a network signed certificate after their authenticity has been warranted by some other members.

According to Kadri.B et al, [3] they propose a secured weight-based clustering algorithm allowing more efficiency, protection and trust in the management of cluster size deviation. This algorithm is called Secured Clustering Algorithm (SCA), since it includes security requirements by using a trust value defining how much any node is trusted by its neighbourhood, and by means of the certificate as node's identifier to avoid any possible attacks (Spoofing). SCA elects cluster-head according to its weight computed by combining a set of system parameters (Stability, Battery, Degree … etc). It also overcomes some limits in existed algorithms by defining new mechanisms as cluster division, merging diminution and extension. SCA forms a hierarchical structure which can be used for both security and routing protocols.

According to Kalaivani.R et al.,[4]Leader is elected based on the residual energy of each node that is enough to run IDS. Too much of resources are wasted for the implementation of intrusion detection scheme for each node. Hence nodes are grouped into cluster and cluster head is elect to serve other node in network, where as selfish node by means of maximum resources are not nominated for cluster head selection, as of self interest to save its

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

own power. Nodes are provided incentives inside the leader election process by VCG mechanism for preventing the nodes from exhibiting the selfish behaviour.
1) To certify security and to detect the intrusion in Mobile Ad hoc networks select a leader from the 1hop cluster as cluster head contains most resource.
2) To avoid the issues arise due to best collection of leader and performance overhead, a solution is Mechanism based design theory.
3) The solution provides nodes by means of incentives in the form of reputations to encourage nodes in honestly participating in the election process.

According to Muneeswari.G et al.,[5] they combine Secured Clustering Algorithm (SCA) and Data fusion to improve security in MANET. Maintaining security in MANET is the critical one since it has several distinct characteristics like low secure state, low processing and radio range, low energy power, mobility and detecting function for limited nodes. In the proposed scheme, they address all these issues by using SCA. SCA elects cluster-head according to its weight which is computed by combining parameters like stability, energy, secure, degree. Since each cluster-head has measurement, more than one device needs to be chosen and their observation can be fused to increase accuracy. The fusion can be done by using Dempster-Shafer which is well suited for an uncertainty problem.

According to Preetida Vinayakray-Jani et al.,[6] proposes architectural security concept in distributed manner where network is divided into clusters with one cluster head node each. This cluster head node also perform as a router providing proactive hidden routing by using Steganographic methods for inter-cluster security. Besides cipher method is used to offer intra-cluster security. The future secure architecture specifies operational view of cluster head as a router that provides trust, anonymity with confidentiality through Steganography and Cryptography respectively.

According to Seunghun Jin et al., [7] they present a new trust evaluation scheme in an ad hoc network. To conquer the limited information about unfamiliar nodes and to reduce the required memory space, they propose a cluster-based trust evaluation scheme, where neighboring nodes form a cluster and select one node as a cluster head. The head issues a faith value certificate that can be referred to by its non-neighbour nodes. In this way, an evaluation of an unfamiliar node's trust can be done very efficiently and precisely.

According to Shubha Mishra et al., [8] they proposed an efficient dynamic clustering protocol for MANET. In dynamic clustering protocol they have five state connections. These are un-clustered state, orphan state, election state, cluster node state, in addition to cluster head state. Also, they develop key distribution method for the distribution of symmetric keys in MANETs. In dynamic clustering protocol they designed to verify the protocol and have an estimate of the cost to gather the density information. For evaluating in terms of time, time used up as part of cluster was measured. From clustering point of view, numbers of clusters, as well as number of nodes per cluster were measured. To calculate approximately the network performance, number of protocol packets, with application packets transmitted were measured.

According to Suganya Devi.D et al.,[10] they propose a new cluster based multicast tree (CBMT) algorithm for secure multicast key sharing, in which source node uses Multicast Destination Sequenced Distance Vector (MDSDV) routing protocol to collects its 1 hop neighbours to form cluster and each node which have child node is elected as the Local controllers of the created clusters.

According to Yao Yu et al, [11]they analyze the security problem in the hierarchical mobile Ad Hoc networks. And then we offer a secure clustering algorithm based on reputation in defence of threats in clustering. In the algorithm, the nodes 'reputation is used to develop security, which is evaluated by combining the experience of the node in the routing process. Additionally, we consider degree and relative mobility in the clustering to guarantee the stability of clusters. The weight of each node is computed from beginning to end considering the above three factors at the same time. It is used to elect the secure backbone nodes in the networks. Moreover, it is efficient in the cluster rebuilding and healing.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

6. CONCLUSION

In this study, various security strategies of clustering in MANET have been visualized**.** The research on MANET security is still in its early stage. Because the solutions are designed explicitly with certain attack models in mind, they work well in the occurrence of designated attacks but may collapse under unanticipated attacks. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities.

REFERENCES

[1]. Avinash Jethi and Seema [2013]: "An approach to Handle Man in Middle Attack in Cluster based Architecture" Elixi Comp.
Sci. & Engg.
[2]. Bechler.M, et al.,[2004]: " A Cluster-Based Security Architecture For Ad Hoc Networks", IEEE INFOCOM .
[3]. Kadri.B et al,[2007]:"Secured Clustering Algorithm for Mobile Ad Hoc Networks", IJCSNS International Journal of Computer
Science and Network Security, VOL.7 No.3,.
[4]. Kalaivani.R et al .,[2013]: "Cluster Based Leader Election and Intrusion Detection System for MANET", Vol 2 Issue 2 February ,
International Journal of Computer Science and Management Research
[5]. Muneeswari.G et al.,[2012]:"Combining Secured Clustering Algorithm &Data Fusion based on Dempster-Shafer Theory to
Enhance Security in MANET", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13.
[6].Preetida Vinayakray-Jani, et al., [2012]:L"Security Architecture for Cluster based Ad Hoc Networks", .
[7] .Seunghun Jin et al.,[2005]:" Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network", ETRI Journal, Volume 27, Number 4,
August 2005.
[8].Shubha Mishra et al.,[2011]:"Efficient Secure Clustering Protocol For Mobile Adhoc Network" Volume 2, No. 9, September 2011,
Journal of Global Research in Computer Science
[9] .Sonia Boora et al., [2011]: "A Survey on Security Issues in Mobile Ad-hoc Networks"IJCSMS, Vol. 11, Issue 02
[10]. Suganya Devi.D et al.,[2009]" Cluster Based Multicast Tree for Secure Multicast Key Distribution in Mobile Adhoc Networks".
[11].Yao Yu, Lincong Zhang [2012]:"Secure Clustering Algorithm in Mobile Ad Hoc Networks", IPCSIT vol. 29.
.