IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. IV (Jul.-Aug. 2016), PP 01-05
www.iosrjournals.org

Challenges and Issues of Cluster Based Security in MANET

Sapna B Kulkarni[1] Dr.Yuvaraju B N[2]
[1] *Research Scholar, VTU University, Belgaum, India*
[2]*Professor, Department Of CSE, NIE, Mysuru, India*

Abstract: *Mobile ad-hoc networks are a specific kind of wireless networks that can be quickly deployed without pre- existing infrastructures. Even though there are various studies on cluster based security in MANET but there is a clear absence of a comprehensive performance study that provides a unified platform for comparing such techniques. Thus in order to provide a better understanding of cluster based security in MANET a brief survey is needed. Hence to the point, outline of the key concept, performance metrics used, as well as the advantages and drawbacks of each discussed mechanism are given. Finally, the comparison table is constructed to show the cluster based security in MANET with method performance metrics, advantages and disadvantages based on trust based security and authentication based security.*

I. Introduction

1.1 MANET

A mobile ad hoc network is a set of wireless nodes which cooperatively form a network independent of any fixed infra structure or centralized administration. MANET is a collection of dynamic mobile nodes which are self-organized and able to communicate without using a pre-existing network infrastructure. Each node acts as personal device and as a router and so it is able to forward data packet to other nodes [1]. MANET nodes have limited processing speed and power, battery, storage, and communication capabilities. MANET is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. The mobility of the routers is provided randomly and organized themselves arbitrarily [2] [3].

Applications:

- Emergency search-rescue operations
- Meeting events
- Conferences,
- Battlefield communication between moving vehicles or soldiers [4] [5].

Issues

- Error-prone channel state
- Hidden problem
- Exposed terminals
- Bandwidth-constrained, variable capacity links
- Energy-constrained operation
- Security Issues [3] [4]

1.2. Trust based security

Routing in MANET is the most challenging task due to its dynamic nature, lack of central control, and restricted resource limitations. Clustering is the process of dividing the network into different virtual groups based on certain rules [8].One of the nodes in cluster is elected as cluster head (CH), which acts as local coordinator for its cluster and take care of inter cluster and intra cluster communication, cluster maintenance and so on. While routing instead of flooding routing information across all nodes in network, clusters restricts the spreading of routing information only to CH and gateway nodes [10] [16].This avoids wastage of resources that occurs due to flooding. Non overlapping clusters may use the same frequency for transmission. Cluster structure maintenance involves additional cluster related information exchange between cluster members and CH [11] [12][13].

1.3Authentication based security

Security is one crucial requirement for these network services. Implementing security is therefore of prime importance in such networks. Provisioning protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to disrupt network security, is a primary concern. Owing to the absence of infrastructure, mobile nodes in a MANET have to implement all aspects of network functionality themselves; they act as both end users and routers, which relay packets for other nodes[13][14].Unlike the conventional network, another feature of MANETs is the open network environment

where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them more vulnerable to various types of security attacks than the wired networks [15] [17] [18]

II. Survey

2.1 Works on Trust based security

Particle Swarm Optimization based secure QoS clustering for MANET

Particle Swarm Optimization [1] based secure QoS clustering for MANET Mobile ad hoc network was a dynamic wireless network of mobile nodes without any centralized control. Energy efficient routing was the most challenging task of MANET. Clustering in MANET gives energy efficient solution. They have proposed a secure clustering algorithm using multi-objective particle swarm optimization technique. The algorithm uses three objective functions based on nodes QoS parameters: trust value, life time and available bandwidth. The main advantage of MOPSO was that it provides multiple solutions at a time through optimal Pareto front. Here they have discussed the performance of the proposed approach by varying number of nodes and transmission range of nodes.

Secure Clustering Algorithm in MANET

Ad Hoc networks were much vulnerable to be attacked because of its characteristics. In this paper, they analyze the security problem in the hierarchical mobile Ad Hoc networks. And then they proposed a secure clustering algorithm [2] based on reputation in defense of threats in clustering. In the algorithm, the nodes reputation was used to improve security, which was evaluated by combining the experience of the node in the routing process. In addition, they consider degree and relative mobility in the clustering to guarantee the stability of clusters. The weight of each node was computed through considering the above three factors simultaneously. It was used to elect the secure backbone nodes in the networks. Moreover, it was efficient in the cluster rebuilding and healing. The simulation results show that the proposed algorithm could effectively improve the security and stability of network.

Secure Reputation-Based Clustering Algorithm for Cluster based energy optimized MANET

They have proposed to analyze the security drawback within the hierarchical mobile ad hoc networks. Then they proposed a secure clustering algorithm [3] supported based on reputation in defense of threats in clustering. In this algorithm, the nodes' reputation was used to improve security of cluster which was evaluated by combining the occurrence of the node in the routing process. In addition, they consider the degree and relative mobility within the cluster to ensure the stability of clusters. The weight of every node was computed through considering the on top of three factors at the same time. It's used to elect the secure backbone nodes within the networks. Moreover, it's economical within the cluster reconstruction and healing, and this proposed work was totally different than other research was working at the time now.

Reputation-Based Clustering Algorithms in MANET

Clustering was one of the main techniques that were used to increase the scalability of MANETs, but without any security considerations clustering was prone to various security attacks. Some cryptographic-based schemes have been proposed to secure the clustering process, but they were unable to handle the internal attacks. Trust-based clustering schemes [4] have combined the trust management systems with the existing state of art clustering solutions and using cryptographic mechanism these schemes presented the most complex and secure clustering solutions that were resilient against both internal and external attackers. They have presented an in-depth analysis of trust-based clustering schemes and illustrate how reputations were integrated in these schemes.

Trust- and Clustering-Based Authentication Services in MANET

A mobile ad hoc network was a kind of wireless communication network that does not rely on a fixed infrastructure and was lack of any centralized control. These characteristics make it vulnerable to security attack, so protecting the security of the network was essential. Like many distributed systems, security in ad hoc networks widely relies on the use of key management mechanisms. However, traditional key management systems were not appropriate for them. This work aims at providing a secure and distributed authentication service in ad hoc networks [5]. They proposed a secure public key authentication service based on their trust model and network model to prevent nodes from obtaining false public keys of the others when there were malicious nodes in the network.

Trust-based Cluster head Selection Algorithm for MANET

Mobile Ad hoc Networks (MANETs) consist of a large number of relatively low-powered mobile nodes communicating in a network using radio signals. Clustering was one of the techniques used to manage

data exchange amongst interacting nodes. Each group of nodes have one or more elected Cluster head(s), where all Cluster heads were interconnected for forming a communication backbone to transmit data. Moreover, Cluster heads should be capable of sustaining communication with limited energy sources for longer period of time. Misbehaving nodes and cluster heads could drain energy rapidly and reduce the total life span of the network. In this context, selection of best cluster heads with trusted information becomes critical for the overall performance. They have proposed Cluster head(s) selection algorithm [6] based on an efficient trust model. This algorithm aims to elect trustworthy stable cluster head(s) that could provide secure communication via cooperative nodes. Simulations were conducted to evaluate trusted Cluster head(s) in terms of clusters stability, longevity and throughput.

III. Works on Authentication based security

Cluster based Key Management Scheme for MANET with Authentication

A Mobile Ad Hoc Network (MANET) was a self organizing, infrastructure less, multi-hop network. The wireless and distributed nature of MANETs poses a great challenge to system security designers. Key management was crucial part of security; this issue was even bigger in MANETs. The distribution of encryption keys in an authenticated manner was a difficult task. Because of dynamic nature of MANETs, when a node leaves or joins it need to generate session key to maintain forward and backward secrecy. In this paper they divide the network into clusters. Cluster head would maintain the group key, it would also update the group key whenever there was a change in the membership and also they provide authentication between communicating nodes both in inter and intra cluster. They have proposed a cluster based tree (CBT) algorithm [1] for secure multicast key distribution, in which source node uses Destination Sequenced Distance Vector(DSDV) routing protocol to collects its1 hop neighbors to form cluster. Simulation results shows the demonstration of CBT using DSDV in terms of end to end delay, key delivery ratio and packet drop rate, fault tolerance, communication cost under varying network conditions.

Cluster-Based MANETs with Threshold Signature

Security supports were a significant factor in the design of security system in ad hoc networks. It was particularly important to protect the identities of individual nodes to avoid personal privacy concerns. In this paper, they proposed a security system for ID-based anonymous cluster-based MANETs to protect the privacy of nodes. Moreover, they proposed a threshold signature scheme without pairing computations, which diminishes the computation load on each node. To the best of their knowledge, their proposed security system was the first in which the pseudonym was combined with cluster-based mobile ad hoc networks [2] without a trusted entity. According to their protocol analysis, their proposal satisfies most properties for an anonymous security system and effectively copes with dynamic environments with greater efficiency by using secret sharing schemes. Therefore, it could be usefully applied to preserve privacy in dynamic MANETs without a trusted entity, such as military battlefields, emergency areas, mobile market places, and vehicular ad hoc networks (VANETs)

Cluster-based Certificate Revocation with Vindication Capability for MANET

Mobile ad hoc networks (MANETs) have attracted much attention due to their mobility and ease of deployment. However, the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge was to guarantee secure network services. To meet this challenge, certificate revocation was an important integral component to secure network communications. They have focused on the issue of certificate revocation to isolate attackers from further participating in network activities. For quick and accurate certificate revocation, they proposed the Cluster-based Certificate Revocation [3] with Vindication Capability (CCRVC) scheme. In particular, to improve the reliability of the scheme, they recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, they proposed the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them.

Clustering Based Certificate Revocation in MANET

They have proposed a scheme for clustering based certificate revocation scheme [4], which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates. However, owing to a limitation in the schemes certificate accusation and recovery mechanism, the number of nodes capable of accusing malicious nodes decreases over time. This could eventually lead to the case where malicious nodes could no longer be revoked in a timely manner. To solve this problem, they proposed a method to enhance the effectiveness and efficiency of the scheme by employing a threshold based approach to restore a node's accusation ability and to ensure sufficient normal nodes to accuse

malicious nodes in MANETs. Extensive simulations show that the method could effectively improve the performance of certificate revocation.

Secure Clustering Protocol for MANET

In their dynamic clustering protocol have five state interactions. These were un-clustered state, orphan state, election state, cluster node state, and cluster head state. Also, they develop key distribution method for the distribution of symmetric keys in MANETs. Their dynamic clustering protocol [5] was designed to verify the protocol and have an estimate of the cost to gather the density information. They did the analysis from their dynamic clustering protocol different perspectives, in terms of time, clustering, and network packets. For evaluating in terms of time, time spent as part of cluster was measured. From clustering perspective, number of clusters, and number of nodes per cluster were measured. To estimate the network performance, number of protocol packets, and application packets transmitted were measured.

Secure Communication Architecture Based Clustering Algorithm for MANET

Mobile ad hoc networks were self created and self organized without the support of network infrastructure, consists of mobile devices, such as laptops, cell phones, etc. Security was one of the prime Issues in ad hoc network due to their rapidly change in topology and mobility of nodes. However, the infrastructure less and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. They have proposed a Secure Communication architecture based on "BBCMS" clustering algorithm [6]. In this algorithm elect cluster head (CH) according to its weight computed by combining a set of system parameters. It also overcomes some limits in Existed algorithms by defining mechanisms as cluster dissection, assimilation. In the proposed system, the overall network was divided into clusters where the cluster-heads (CH) were connected by virtual networks. For secure data transmission, credential authority (CA) issues a certificate (X.509) to the requested node for authentication. The certificate of a node was renewed or rejected by CH, based on its trust counter value.

IV. Comparison table of existing works

Name of the work	Contribution	Performance Metrics	Advantages	Disadvantages
Trust based Security				
Particle Swarm Optimization based secure QoS clustering for MANET	Optimization based secure QoS clustering	Number of nodes	Multiple solution at a time	Security problem over clustering
Secure Clustering Algorithm in MANET	Secure Clustering in MANET	Packet delivery ratio, sending packet ratio, overhead	Improved cluster structure	Decrease in Network performance
Secure Reputation Based Clustering Algorithm for Cluster based energy optimized MANET	Secure Reputation-Based Clustering	Confidentiality, Data Integrity, Authentication, Non-repudiation:	Improves turnout of the network	lot of vulnerability in ad hoc networks, creating the problem of security problem and difficult
Reputation-Based Clustering Algorithms in MANET	Secure Reputation-Based Clustering	Trust value	Trust values proved to be the best	Lack of solution to operate in both secure and hostile environment
Trust and Clustering Based Authentication Services in MANET	Clustering Based Authentication Services	Orphan time, Election time and Clustered time.	Secure exchange and efficient storage	consume a huge amount of network bandwidth, cause rapid energy drain
Trust-based Cluster head Selection Algorithm for MANET	Trust-based Cluster head Selection	Cluster stability, longevity and Throughput	Provide secure communication via cooperate nodes	The way the message is passed through may overload the cluster head
Authentication based Security				
Cluster based Key Management Scheme for MANET with Authentication	Cluster based Key Management for authentication	End To End Delay, Key Delivery Ratio And Packet Drop Rate, Fault Tolerance, Communication Cost	Improved performance metrics	Issue of average end to end delay to achieve an efficient key distribution process
Cluster-Based MANETs with Threshold Signature	Cluster-Based signature using threshold	Correctness, performance, Security	To preserve privacy in dynamic MANETs without a trusted entity	Unresolved Security issues
Cluster-based Certificate Revocation with Vindication Capability for MANET	Cluster-based Certificate Revocation	Revocation time, accuracy	Revocation scheme is effective and efficient to guarantee secure communication	More vulnerable to various types of security attacks than the wired networks
Clustering Based Certificate Revocation in MANET	Cluster-based Certificate	Detection time, Number of nodes, mobility	Revoke the certificates of malicious nodes	Gradually Reduced number of Normal nodes

	Revocation	model, node placement, routing protocol, pass time	promptly and accurately	
Secure Clustering Protocol for MANET	Secure Clustering	Failure rate, successful rate	Network endures malicious nodes that issue false certificates	High unreachable rate
Secure Communication Architecture Based Clustering Algorithm for MANET	Secure Communication based clustering	Belief value, connectivity, stability, Mobility	High security to the network	Subjected to various attacks

V. Conclusion

In this paper, a various analysis on cluster based security in MANET has been studied. The exiting survey related to the proposed study is discussed. Then based on the techniques used the following properties has been discussed such as performance metrics, list the advantages and limitations. Finally from the comparison of existing works we have summarized the trust based security and authentication based security. This can be helpful in developing new techniques by understanding the existing techniques in future

References

[1]. Sandeep Kr. Agarwal, Amit Garg and K. V. Arya, "Security Issues & Clustering Based Solutions in Mobile Ad-hoc Networks - A Survey," Journal of International Academy of Physical Sciences, Vol. 16, pp. 295-308, 2012

[2]. Avinash Jethi and Seema, "Cluster Based Security Architecture in Wireless Ad-Hoc Networks: An Overview," Journal of Global Research in Computer Science, Vol. 2, 2011

[3]. Chandra Prakash, Kunal Jain, and Priyanka Tripathi, "A Comparative Study of Intrusion Detection System forWireless Sensor Network," International Journal of Advance Foundation and Research in Computer (IJAFRC), Vol. 1, 2014

[4]. J. Godwin Ponsam and R.Srinivasan, "A Survey on MANET Security Challenges, Attacks and its Countermeasures," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 3, 2014

[5]. K. Gomathi, B. Parvathavarthini, "An Exclusive Survey on Cluster Based Key Management Techniques in MANET," International Journal of Engineering Development and Research, 2014

[6]. M. Anupama and Bachala Sathyanarayana, "Survey of Cluster Based Routing Protocols in Mobile Adhoc Networks," International Journal of Computer Theory and Engineering, Vol. 3, No. 6, 2011

[7]. Abdelhak Bentaleb, Abdelhak Boubetra, Saad Harous, "Survey of Clustering Schemes in Mobile Ad hoc Networks, Communications and Network, Vol. 5, pp. 8-14, 2013

[8]. MerinAchankunju, R. Pushpalakshmi,and A.Vincent Antony Kumar, "Particle Swarm Optimization based secure QoS clustering for Mobile Ad hoc Network," In proceedings of : International conference on Communication and Signal Processing, 2013

[9]. Yao Yu &Lincong Zhang, "A Secure Clustering Algorithm in Mobile Ad Hoc Networks," In proceedings of : 2012 IACSIT Hong Kong Conferences, Vol. 29, 2012

[10]. Keshav Kumar Tiwari and Sanjay Agrawal, "A Secure Reputation-Based Clustering Algorithm for Cluster based energy optimized Mobile ad-hoc network," International Journal of Advanced Research in Computer Science and Software Engineering,Vol. 3, 2013

[11]. MoazamBidak and Mohammad Masdari, "Reputation-Based Clustering Algorithms in Mobile Ad Hoc Networks," International Journal of Advanced Science and Technology, IEEE 12th International Workshop, Vol. 54, 2013

[12]. Edith C. H. Ngai and Michael R. Lyu, "Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks," In proceedings of :Distributed Computing Systems Workshops, pp. 582 - 587, 2004

[13]. Raihana Ferdous, VallipuramMuthukkumarasamy, and ElankayerSithirasenan, "Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks," In proceedings of : 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE , pp. 589 - 596, 2011

[14]. Gomathi K. and Parvathavarthini B., "An Efficient Cluster based Key Management Scheme for MANET with Authentication," In proceedings of : Trendz in Information Sciences & Computing (TISC), pp. 202 - 205, 2010

[15]. YoHan Park, YoungHo Park, and SangJae Moon, "Anonymous Cluster-Based MANETs with Threshold Signature," International Journal of Distributed Sensor Networks, 2013

[16]. Wei Liu, Nishiyama, H., Ansari, N. and Jie Yang , "Cluster-based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks," Journal of Parallel and Distributed Systems,, Vol. 24, pp. 239 - 249, 2013

[17]. V. Anil Kumar, K.Praveen Kumar Rao, E.prasad, and N.Gowtham Kumar, "Clustering Based Certificate Revocation in Mobile Ad Hoc Networks," International Journal of Computer Science and Management Research, Vol. 2, 2013

[18]. Shubha Mishra and Dr. Manish Shrivastava, "Efficient Secure Clustering Protocol For Mobile Ad-Hoc Network," Journal of Global Research in Computer Science, Vol. 2, 2011