ISSN No. 0976-5697

Volume 2, No. 4, July-August 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Robust Authenticated Clustering Strategies for Mobile Ad hoc Networks (MANETs)

Shruti Sangwan*
Department of Computer Science & Engineering
UIET, Kurukshetra University, Kurukshetra
Haryana, India
ssshrutisangwan8@gmail.com

Nitin Goel
Department of Computer Science & Engineering
UIET, Kurukshetra University, Kurukshetra
Haryana, India
goelnitin0887@gmail.com

Ajay Jangra
Department of Computer Science & Engineering
UIET, Kurukshetra University, Kurukshetra
Haryana, India
er_jangra@yahoo.co.in

Abstract: Mobile Ad-hoc Network is a wireless network with self-configuring nodes which forms a temporary network without any centralized administration such as servers and base stations. One of the most critical issues in these networks is the deployment of adaptive, extensible and flexible authentication and access control policies. Moreover, the lack of structured hierarchy in MANETs complicates the overall task of implementing these policies. The network performance might be improved if the network is clustered by grouping together nodes that are in close proximity. In the present paper our primary goal is to provide both an adaptive authentication system and a clustering scheme for MANET keeping the clustering latency, cost and performance in mind.

Keyword: Security, Authentication, Cluster, Mobile Ad hoc Networks (MANETs), Fair Routing

I. INTRODUCTION

The mobile ad hoc network (MANET) is established by a group of mobile and independent nodes connected by wireless links. These associated hosts are independent to roam in an arbitrary motion. The unavailability of controller coupled with the frequent changes in the network topology makes network functions or services in MANET much complicated as compared to that in any other network. The structure of mobile ad hoc network is decentralized and communicating nodes are heterogeneous; some nodes may have different processing capabilities and battery power. The nodes are responsible of not only forwarding packets for other nodes but also perform extensive computation. These computations can be in terms of route maintenance, key management and the deployment of security schemes. The transmissions and computations cause the resources to be depleted. Therefore, to avoid a node dropping out of the network prematurely, the overhead of all the activities and deployed schemes should be kept to a minimum. To deal with the random entries of nodes, security mechanisms need to be robust and flexible to some extent. [2,7]

II. AUTHENTICATION

Authentication is one of the most remarkable security aspects in any system because all the remaining attributes (i.e. integrity, confidentiality, availability) depends completely on it. An efficient authentication scheme with in a network guarantees the right identities of users; to be able to identify a node and to be able to prevent impersonation. It is possible to implement a Central authority (CA) at a point such as a router, base station or access point in wired networks to solve authentication problem. But in MANETs, there is no central authority and it is much difficult to authenticate an entity to ensure security among nodes for communication. Mobile ad hoc network poses some of the unique characteristics like lack of structured hierarchy and frequent route modifications.

The lack of limited physical protection of broadcast medium makes the network more vulnerable to security attacks. An environment where nodes are highly dynamic and the topology changes are highly frequent, authentication and access control policies must be adaptive according to the network behavior. Mobility pattern of nodes is usually crucial to the network performance as protocol may exploit the mobility to obtain advantages in many important aspects of ad hoc networks, such as network capacity, security and information dissemination. Ad hoc networks are self configured with no infrastructure, no central authority, no centralized trusted third party, no central server and no secret share dealer, even in the initialization phase of the network. A static approach in such a scenario isn't feasible and periodic assessment of the nodes is must.[13].

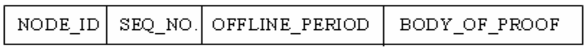
An efficient system model should scale to any sort of networks with different levels of topology changes and bandwidth of connections. To grade a node to be authenticated, co-ordination among rest of the network entities provides a means to detect its behavior. Nodes' authenticity is questioned every time it requests to establish a connection after a predefined time interval. Computation and strong storage capacities of nodes affect the network services as well as enforced mechanisms. The lesser is the overhead more will be the throughput of a mobile node. Trusting the node before forwarding the data and routing packets ensures security and thus reliability of connections. The malicious, selfish and unauthenticated entities violate the protocols and disrupt the communication either actively or passively. To avoid such scenarios the identity of a node must be verified before allowing it to participate in the network operations. Trusted nodes not only guarantees security but a co-operative environment as well. Successful and efficient authentication in mobile ad hoc networks are critical for assuring secure and effective operation of the supported application, especially in distributed field applications where mobile nodes are spread over a large geographical region. Various certificate-based authentication mechanisms have been proposed for MANETs.

The main barrier when providing the security mechanisms is the set of restrictions associated to computational, communication and power supply resources present in this environment Nevertheless, there are also other intrinsic features that increase this difficulty. The mobility of the nodes produce continuous nodes insertions and deletions and so, the continuous instances of the authentication protocol are developed. As a result, designing scalable solutions here is a must.[1]. Furthermore, it should be borne in mind that there is not any fixed infrastructure, so the security solutions should admit that legitimated nodes carry out all the required tasks, including routing and entity authentication, in a self-organized and self-controlled manner. The limitations on the network transmission range is the another problem to be considered and to develop secure routing mechanisms is of vital importance. Mobile ad hoc networks are vulnerable to attacks due to the lack of any specific boundary and random entry of nodes in the network. Authentication is the hallmark of security and failure to achieving this so far is a stumbling block in the way of securing MANET. At small scale the authentication can be managed by the nodes through handshaking but at larger scale it becomes complex and demands the involvement of a Trusted Third Party (TTP). Some of the proposed schemes are either based on self-organization in MANETs without TTP where the identity is resolved by independent nodes themselves and some are based on absolute TTP , while a hybrid form can also be used. The design of authentication scheme must ensure independence from protocol, design extensibility and flexibility according to the application.[8,15]

III. AUTHENTICATION SCHEME

The insertion of a new node starts with persuading a legitimate node. The non-legitimate node requests for its insertion into the network through a request message which includes its node ID, sequence number, off line period and body of proof. Sequence number is included so as to identify multiple requests from the same node and to avoid the loops. The legitimate node checks for the node-id, whether the ID carried by this non-legitimate node is unique in its close proximity or not. This legitimate node investigates the past behavior of it before allowing this node for the services of the network. Investigation includes the information regarding the nodes' mobility and its co-operation in the network operations.[4]. The algorithm needs to ensure the exclusion of malicious and selfish nodes. Misbehaving nodes do not co-operate in the network operations either intentionally as they conserve their resources or unintentionally, when do not have the sufficient resources to participate in the network operations. The legitimate node forwards the investigation message (INVES_MSG) to its neighbors (i.e. to the nodes in its transmission range). This broadcasting of messages is the limited broadcasting i.e. the packets are flooded to the neighboring nodes. Upon receiving the INVES_MSG neighbor nodes checks their locally maintained information to detect the routing pattern followed by the requesting non-legitimate node earlier. The replies (INVES_REP) are collected and further analyzed at the node from where the INVES_MSG originated. The performance and reliability of the requesting or non-legitimate node are the two important parameters which decide their legitimacy.[12]

Request message from the non- legitimate node

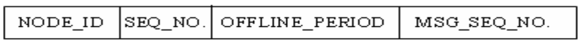


NODE_ID	SEQ_NO.	OFFLINE_PERIOD	BODY_OF_PROOF

Figure 1. Request Message Packet

Sequence number information (SEQ_NO.) eliminates the formation of loops in the network and to differentiate between the recent and the stale requests. Offline period denotes the time interval when the node is out of coverage. If a node has been off-line and wants to connect on-line, it has to contact a legitimate node who checks whether the off-line period is not greater than Θ, where Θ (theta) denotes a predefined time interval which depends on the number of nodes, computing power of nodes and the connections bandwidth. Body_ of_ proof is to confirm the presence of all the legitimate nodes in an active way by broadcasting their body of proofs every certain interval of time to all the legitimate nodes.

A. Legitimate requested node checks the information if ((OFFLINE_PERIOD < Θ) && (SEQ_NO. = unique))
Allow the node
else if((OFFLINE_PERIOD > Θ) && (SEQ_NO. = unique))
Send INVES_MSG



NODE_ID	SEQ_NO.	OFFLINE_PERIOD	MSG_SEQ_NO.

Figure 2. Investigation Message Packet

else discard the request

B. For every neighbor node process INVES_MSG

a. For the given node ID check the mobility and the routing patterns.

b. INVES_REP is forwarded to the node which initiated the INVES_MSG.

C. After receiving enough replies carry out a probabilistic analysis.

D. Send a reply message to the requesting node. Send the topology information to the node if it is legitimate now.

E. Re-evaluate the body of proof for every node in the network after T time interval.

Where: T depends upon the no. of nodes and throughput of the network.

a. Cost = No. of messages involved * length of each message.

b. Authentication latency= Delay between the time when the request message was sent and the time when the node receives the reply.

c. Body of proof= Mobility information and the no. of routes through this node to the no. of packets delivered.

IV. CLUSTERING: FORMATION OF CLUSTER AND DESIGN PARADIGMS

Due to the unavailability of a central controller and limited battery power, a flat structure may not be the efficient organization for routing between nodes in the case of large MANETs. One of the way support efficient communication and improved system performance is to develop wireless backbone architecture. Such networks may be logically represented as a set of clusters by grouping together nodes that are in close proximity. The formation of clusters and the organization of nodes in such a manner, with a view to improve the efficiency of routing, incurs low cost in terms of the resources used such as bandwidth, battery power, computation power etc. the purpose of clustering may be defeated otherwise. Certain nodes are elected to form the wireless backbone. These nodes are called Cluster heads and Gateways while other nodes work as member nodes.[3].

A Cluster head serves as a local co-coordinator for its cluster and vested with the responsibility of routing, data forwarding and so on, for all the nodes within its cluster. Gateways nodes are the nodes at the fringe of a cluster within inter-cluster links and access the neighboring cluster to forward information between clusters. A neighboring cluster is accessed through the gateway nodes.

A cluster member is a node other than a cluster head. It might behave as a cluster gateway if present at the boundaries of the cluster. These member nodes form the communication links within a cluster and may access Cluster head for its services. The Clusters are either deployed with proactive routing scheme or a reactive routing scheme and thus operates accordingly. Nodes are powered by limited batteries because of their mobile nature. Cluster head is involved in every communication within its cluster, so the amount of communication should be kept to a minimum to avoid a node to be dropped out of the network prematurely. The bottleneck to the functioning of a cluster head must be eliminated.

V. THE DESIGN PARADIGMS FOR BUILDING AN OPTIMIZED CLUSTERED ARCHITECTURE

A. Reliable Inter-Cluster Links:

Once the connections are set up, the effects of mobility of nodes should be kept at minimum. Higher node mobility results in high cost due to the reconfigurations. Mobility based and weighted clustering scheme have been proposed which supports the formation of highly connected intra-cluster links and takes mobility as the metric for cluster formation. The nodes moving with same velocity are grouped together to form a cluster, but the velocity with which the node moves is not the only factor to consider, their direction of movement also has important concerns. Cluster formation and maintenance are expensive tasks for the nodes so there should be minimum re-configurations and re-affiliations when a node detach from one cluster and attach to another.[5]

B. Low Cluster Head Overhead:

The Cluster head dissipates more power as compared to any other node in the cluster since all the inter-cluster packet forwarding and routing happen through it. The life span of a Cluster head is shorter than the rest of the member nodes.

To avoid its premature elimination from the network, the work load should be minimized. One of the proposed self organized clustering schemes includes the use of a proactive routing protocol such as DSDV within the cluster. The cluster formation and maintenance can be handled using member nodes as each node has its proactively maintained routing information with it. This lowers the overhead of explicit message passing through the cluster head.

C. Low Cost:

The cost in Mobile ad hoc network is determined by the power consumption and message overhead during the construction of a cluster and its maintenance. Energy is a critical resource for every node. A simple cluster formation algorithm begins with the selection of the neighbors for each node (i.e. nodes within its transmission range). Each node diffuses its identity through a HELLO message which is recorded by all the other nodes. This process repeats for all the nodes not yet assigned to any cluster. Moreover, due to the dynamic nature, the nodes and the Clusterhead tend to move in random directions causes a disorganization of the network configuration. Thus the system must be updated from time to time. The communication overhead tends to increase in the lack of an efficient scheme.[10]

D. Low Cluster Latency:

The formation of a cluster and the election of a clusterhead require co-ordination among the mobile nodes. The implemented scheme ensures a minimum latency while forming the clusters. When a node send a request message there occurs a specific delay in receiving a reply message. Also the election of clusterhead puts a significant overhead. All the parameters for the selection of a clusterhead must be evaluated first, and then the cluster ID (CID) is forwarded to all the member nodes. Due to the lack of central entity, mobile node experiences certain delays. This issue has been of considerable interest in the network research community when it comes to infrastructure less networks. Large cluster latencies degrade the throughput and efficiency of the system.[13]

E. Self Organization:

Completely distributed nature and the absence of a centralized infrastructure make it difficult to control the topology of Ad hoc networks. Thus the network is divided into clusters, which has made the situation less complicated. A self organized and self configurable system is one which organizes itself without any external or central dedicated control entity. Self organization is one of the prominent features of a clustered architecture. One of the proposed self organized approaches to MANET clustering includes the use of a proactive inter-cluster routing protocol. Whenever a new node joins the cluster it starts advertising itself and all nodes in its cluster will have an entry for this node in their routing tables after a short time. The system activation and update policies work in two cases:

a. When reviewing cluster formation
b. When a node changes its affiliations from one Clusterhead to a new one.

VI. CLUSTERING SCHEME

In our proposed clustering scheme the proactive routing is implemented as inter-cluster routing scheme. This approach supports all the design paradigms discussed above to its best. The proactive scheme for routing is implemented within a cluster so as to lower down the burden over the clusterhead. This proposal keeps the mobility, resources and hence the throughput of the cluster as the parameters for the construction of a cluster. Cluster architecture is determined by the throughput value of a cluster which is a function of nodes' mobility and its resources. The number of nodes (N) has significant impact on the system performance. Larger the value of N more will be the inter-cluster routing overhead, small values of N defeats the purpose of cluster clustering.[9].

Mean end-to-end delay, a measure shows that how long is the duration time for a packet being generated by source to it being received by the receiver, which includes route discovery latency, retransmission delays, etc. should be low. If the requested node finds the throughput to an acceptable level, it replies the free node with the cluster ID and the other topological information and the routing data. The ID of the newly entered node is then forwarded to the entire member node as well as to the clusterhead. The broadcasted ID when reaches a node in the cluster it makes an update in its routing table to ensure its presence. As shown in the Fig.3 below, the free node sends a request message to node 7 which belongs to the requested cluster. Request message includes the node's ID, mobility and resource information. Node 7 in turn computes the throughput metric as every node maintains the proactive information regarding other nodes in the cluster. A reply message with ClusterID (CID) and topology information of the requested cluster is generated by the requested node (node 7) to the requesting free node after computing the throughput value as shown in the Fig.4 below. The corresponding information is updated at every member node as well as at the clusterhead (node 1).

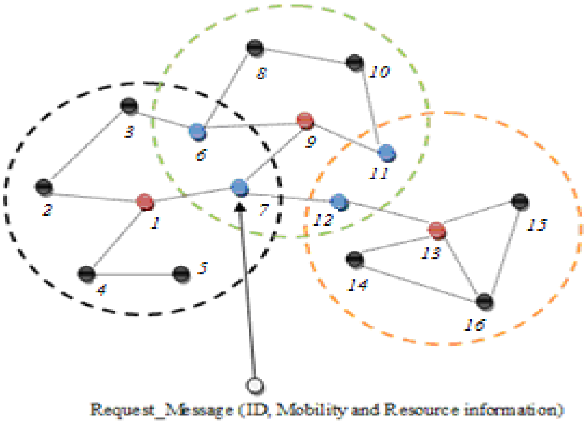
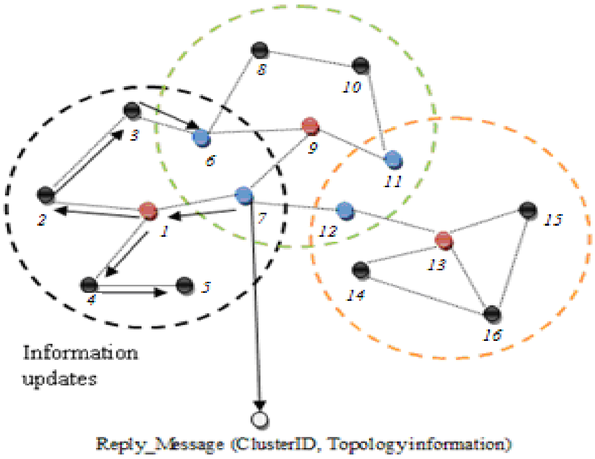
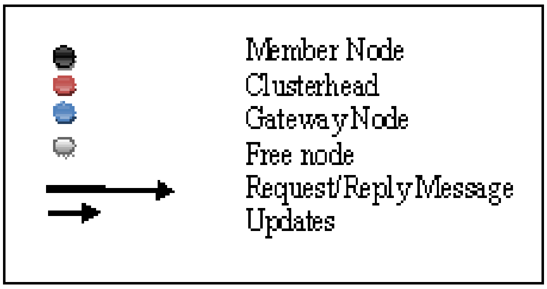
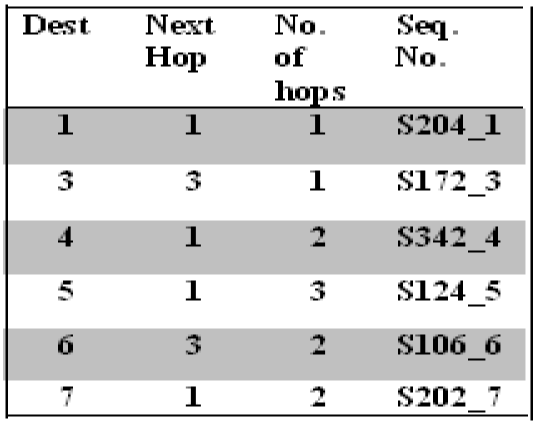


Figure 3. A free node sending a request message.



. Figure 4. A reply generated by the requested node and information update messages at every other node.





Dest	Next Hop	No. of hops	Seq. No.
1	1	1	S204_1
3	3	1	S172_3
4	1	2	S342_4
5	1	3	S124_5
6	3	2	S106_6
7	1	2	S202_7

Table 1. Routing Table of Node 2 at One Instant.

VII. CONCLUSION

The proposed authentication system is able to react to highly dynamic networks where the topology changes are frequent without the requirement of centralized authority. The re-evaluation of the behavior of all the legitimate nodes is carried out in an active way for every specified interval of time. The clustering scheme is ecologically aware as invoke minimum messages and improves the overall performance by considering throughput of the network as the core parameter. Pre-emptive routing avoids the requirement of the knowledge of the entire network for clustering. The present scheme is reliable and efficient as the metric involves mobility and the resource information of a node.

VIII. REFERENCES

[1] P. Caballero-Gill, C. Caballero-Gill, J. Molina-Gill, and A. Quesada-Arencibia, "A Simulation Study of New

Security Schemes in Mobile Ad-Hoc NETworks", ©Springer-Verlag Berlin Heidelberg 2007.

[2] Shruti Sangwan, Ajay Jangra and Nitin Goel "Vulnerabilities And Solutions: Mobile Ad Hoc Networks (Manets) For Optimal Routing And Security" in JGRCS, May 2011

[3] Nevadita Chatterjee, Anupama Potluri and Atul Negi, "A Self-Organising Approach to MANET Clustering".

[4] Rachida Aoudjit, Mustapha Lalam, Abdelaziz M' zoughi, "Load Balancing: An Approach Based on Clustering in Ad Hoc Networks", ©Journal of Computing and Information Technology, 2009.

[5] C.Siva Ram Murthy & B.S Manoj, "Mobile AdHoc Networks- Architecture & protocols", Pearson Education, New Delhi, 2004.

[6] R. Pandi Selvam and V.Palanisamy, "Stable and Flexible Weight based Clustering Algorithm in Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 2 (2) , 2011,824-828.

[7] Ajay Jangra, Nitin Goel & Priyanka "Efficient Power Saving Adaptive Routing Protocol (EPSAR) for MANETs using AODV and DSDV: Simulation and Feasibility Analysis" in IEEE, IPTC 2011

[8] Vasiliou, A., Economides, A.A.: Evaluation of multicasting algorithm in MANETs. In: Proceedings of World Acadmy of Science, Engineering and Technology, vol. 5 (April 2005); ISSN 1307-6884

[9] Y.C. Hu, A. Perrig and D.B. Johnson, "Packets leashes: a defense against wormhole attacks in Wireless networks", in proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Soieties, vol. 3, pp. 1976-1986, San Francisco, Calif, USA, March-April 2003.

[10] Atef Z. Ghalwash, Aliaa A. A. Youssif, Sherif M. Hashad and Robin Doss, "Self Adjusted Security Architecture for Mobile Ad Hoc Networks (MANETs)" 6th IEEE/ACIS, ICIS 2007, IEEE

[11] Feng Li and Jie Wu, "Authentication Via Ambassadors: A Novel Authentication Mechanism In Manets" by NSF grants CNS 0422762, CNS 0434533,CNS 0531410, and CNS 0626240.c 2007 IEEE.

[12] Kavitha Ammayappan, V.N.Sastry and Atul Negi, "Cluster based Multihop Security Protocol in MANET using ECC", 2007 IEEE

[13] Li Wang and Fei Gao, "A Secure Clustering Scheme Protocol for MANET", 2010 International Conference on Multimedia Information Networking and Security, IEEE

[14] K.Gomathi and B.Parvathavarthini, "An Efficient Cluster based Key Management Scheme for MANET with Authentication, 978-1-4244-9008-0/10 ©2010 IEEE, pp. 202-205

[15] Anssi P. Kärkkäinen, "Improving Situation Awareness in Cognitive Networks Using the Self-Organizing Map", International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), Miami Beach, FL, 2011 IEEE.