Volume 4, Issue V, May 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

A Review on Security Issues and its Countermeasures in Mobile Ad-hoc Network

Pooja Sharma[1], Seep Sethi[2]

[1]M.Tech Student, ECE deptt., [2]Assistant Professor, ECE deptt.
S(PG)ITM, Rewari
[1]poosharma00@gmail.com, [2]seep.sethi@gmil.com

Abstract*: In mobile ad-hoc network (MANET), a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time. Due to lack of centralized control, the condition of making routing secure in mobile ad hoc networks is much more challenging than the security in wired network or infrastructure based networks. Mobile ad hoc networks can work properly only if the participating nodes cooperate in routing and forwarding. In this paper, we have surveyed security requirements and various attacks that can affect the overall routing strategy.*

1. INTRODUCTION

Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes [1]. Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engaging themselves in multihop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network [2]. In mobile ad-hoc network, there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets; so there is need of a routing procedure. This is always ready to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes [3].

1.1 Properties of Ad-Hoc Routing protocols

The properties that are desirable in Ad-Hoc Routing protocols are [4]:

***i) Distributed operation*:** The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The dissimilarity is that the nodes in an ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.

***ii) Loop free*:** To improve the overall performance, the routing protocol should assurance that the routes supplied are loop free. This avoids any misuse of bandwidth or CPU consumption.

***iii) Demand based operation*:** To minimize the control overhead in the network and thus not misuse the network resources the protocol should be reactive. This means that the protocol should react only when needed and should not periodically broadcast control information.

***iv) Unidirectional link support*:** The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

v) Security: The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network.

***vi) Power conservation*:** The nodes in the ad-hoc network can be laptops and thin clients such as PDA_s that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.

***vii) Multiple routes*:** To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

***viii) Quality of Service Support*:** Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for. It could be for instance real time traffic support.

1.2 Problems in routing with Mobile Ad hoc Networks :

i). Asymmetric links: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network

***ii). Routing* Overhead:** In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

***iii). Interference*:** This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

***iv). Dynamic Topology*:** Since the topology is not constant; so the mobile node might move or medium characteristics might change. For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks.

2. SECURITY GOALS AND SECURITY THREATS

To secure the routing protocols in MANETs, researchers have considered the following security services: *availability*, *confidentiality*, *integrity*, *authentication* and *non-repudiation* [3][10][15].

i) Availability guarantees the survivability of the network services despite attacks. A Denial-of-Service (DoS) is a potential threat at any layer of an ad hoc network. On the media access control layer, an adversary could jam the physical communication channels. On the network layer disruption of the routing operation may result in a partition of the network, rendering certain nodes inaccessible. On higher levels, an attacker could bring down high-level services like key management service.

ii) Confidentiality ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications. Routing information must also remain confidential in some cases, because the information might be valuable for enemies to locate their targets in a battlefield.

iii) Integrity ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

iv) Authentication enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information.

v) Non-repudiation ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

The networking environment in wireless schemes makes the routing protocols vulnerable to attacks ranging from passive eavesdropping to active attacks such as impersonation, message replay, message littering, network partitioning, etc. Eavesdropping is a threat to confidentiality and active attacks are threats to availability, integrity, authentication and non-repudiation. Nodes roaming in an ad hoc environment with poor physical protection are quite vulnerable and they may be compromised. Once the nodes are compromised, they can be used as starting points to launch attacks against the routing protocols. Most severe threat to mobile ad-hoc network are following:

2.1 Wormhole Attack: The wormhole attack [8] is a severe type of attacks in which two malicious nodes can forward packets through a private "*tunnel*" in the network as shown in Figure 1.

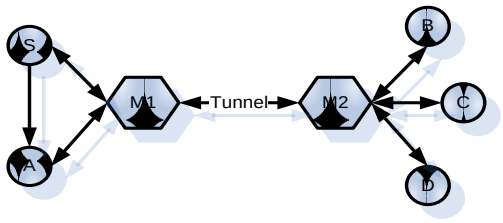

Figure 1: An example of wormhole attack [18]

Here, M_1 and M_2 are two malicious nodes which link through a private connection. Every packet that M_1 receives from the network is forwarded through "*wormhole*" to node M_2, and vice versa. This attack disrupts routing protocols by short circuiting the normal flow of routing packets. Such a type of attack is difficult to detect in a network, and may severely damages the communication among the nodes. Such an attack can be prevented by using *packet leashes* [18], which authenticate the timing information in the packets to detect faked packets in the network.

2.2 Black Hole Attack: In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in DSR, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. As for gray hole, its behavior is similar to a black hole. A gray hole does not drop all data packets but just part of packets. We define the *Gray Magnitude* as the percentage of the packets which are maliciously dropped by an attacker [4]. For example, a gray hole is gray magnitude of 60% will drop a data packet with a probability of 60% and a classical black hole has a gray magnitude of 100%. Fig. 3 shows an example of a black hole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other node's sequence numbers, the source node S will choose the route that passes through node A.

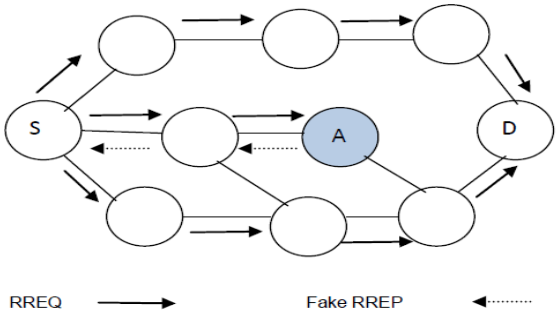

Figure 3: Example of a Black Hole Attack on DSR.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

3. RELATED WORK

Several works propose monitoring schemes to generate trust values describing the trustworthiness, reliability, or competence of individual nodes. Secure routing is an important issue in MANETs. A particularly devastating attack in wireless networks is the black hole attack. The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other nodes without centralized authorities. As a result, an efficient algorithm to detect black hole attack is important. In this paper [1], to improve the quality a modified design of trust based dynamic source routing protocol is proposed. Each node would evaluate its own trusted parameters about neighbors through evaluation of experience, knowledge and recommendations. This protocol discovers multiple loop-free paths which are evaluated by hop count and trust. This judgment provides a flexible and feasible approach to choose a shortest path in all trusted path. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance. The author also compares the simulation results of with and without the proposed secure trust based model. The simulation results demonstrate that the PDR for STBDSR falls from 92% to 80%.A mobile ad-hoc network is a self-configuring network of mobile hosts connected by wireless links which together form an arbitrary topology. Due to lack of centralized control, dynamic network topology and multihop communications, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security in infrastructure based networks. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks. This paper [2] presents a survey of trust based secure routing protocols for mobile ad hoc networks. Different trust based secure routing protocols are discussed and analyzed in the paper along with their strengths, weaknesses and future enhancements.

Theodora kopoulos and Baras [5] analyze the issue of evaluating the trust level as a generalization of the shortest-path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. They consider that nodes use just their own information to establish their opinions. The opinion of each node includes the trust level and its precision. The main goal is to enable nodes to indirectly build trust relationships using exclusively monitored information.

Moe *et al.* [6] proposed a trust-based routing protocol as an extension of DSR based on an incentive mechanism that enforces cooperation among nodes and reduces the benefits that selfish nodes can enjoy (e.g., saving resources by selectively dropping packets). This work is unique in that they used a hidden Markov model (HMM) to quantitatively measure the trustworthiness of nodes. In this work, selfish nodes are benign and selectively drop packets. Performance characteristics of the protocol when malicious nodes perform active attacks such as packet modifications, identity attacks, etc., need to be investigated further. Sun *et al.* [7] proposed trust modeling and evaluation methods for secure ad hoc routing and malicious node detection. The unique part of their design is to consider trust as a measure of uncertainty that can be calculated using *entropy*. In their definition, trust is a continuous variable, and does not need to be transitive, thus capturing some of the characteristics of trust in MANETs. However, this work considers packet dropping as the only component of direct observations to evaluate trust.

Balakrishnnan *et al.* [8] developed a trust model to strengthen the security of MANETs and to deal with the issues associated with recommendations. Their model utilizes only trusted routes for communication, and isolates malicious nodes based on the evidence obtained from direct interactions and recommendations. Their protocol is described as robust to the recommender's bias, honest-elicitation, and free-riding. This work uniquely considered a context-dependency characteristic of trust in extending DSR. A Combiner computes the final trust in a node based upon the information it receives from the Trust and Reputation agents. Trust is computed using direct and indirect information. The trust value is propagated by piggybacking the direct trust value of the nodes along with RREQ packets [9]. The Trust-embedded AODV (T-AODV) routing protocol [10] was designed to secure an ad hoc network from independent malicious nodes by finding a secure end-to-end route. In this protocol, trust values are distributed to the nodes a priori. In the route discovery phase the RREQ packet header contains a trust level field, in addition to the other fields. In [11], the authors have designed a secure routing protocol, called Trust based multi path DSR protocol, which depends on two-way effort of the node by embedding trust to find an end-to end secure route free of misbehaving nodes. This protocol has a drawback routing overhead is very high compared to traditional DSR due to broadcasting of RREQ packet.

4. PROPOSED METHODOLOGY

1. In this work, we are proposing a secure routing technique to deliver the data packets from source to destination.
2. In this technique, we have added nodes faith values according to its cooperation in delivering data packets.
3. For each node in the network, a faith value will be stored that represent the value of the faithfulness to each of its neighbor nodes. We will supply this value to each and every node in the network.
4. It will range from 0.1 to 1. 0.1 faith value means that the node will be preferred least to transfer data packets from source to destination. 0.1 faith value also indicates that the node is a malicious node that can harm the packet. 0.2, 0.3 indicates that these are selfish nodes and 1 indicates that the node will definitely transfer data packets. . If a node starts transferring data to neighbour nodes, then the faith value of that node will be incremented by 0.1.
5. We have applied dijkstra algorithm to find out the shortest route or path from source to destination.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

6. We have supplied three input parameters to dijkstra algorithm. Source node, Destination node and nodes faith values.
7. We can calculate shortest path based on faith values and total distance or cost by using Dijkstra algorithm .

5. CONCLUSION

Security is an important issue in mobile ad-hoc network. Various algorithms have been proposed till now to secure the routing in mobile ad-hoc network, but there is still need for improvement. In this paper, we propose a new approach in dynamic source routing (DSR) protocol based on relationship among the mobile nodes which makes them to cooperate in an infrastructure-less environment. The faith unit is used to calculate the faith values of each node in the network. The proposed algorithm will be helpful in avoiding blackhole node.

REFERENCES

[1] Poonam, K. Garg, M. Misra, "Trust Enhanced Secure Multi-Path DSR Routing" International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010 .

[2] K.Selvavinayaki, K.K.Shyam Shankar, Dr.E.Karthikeyan "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs" International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010

[3] Li, Xin; Jia, Zhiping; Wang, Haiyang;"Trust-based On-demand Multipath Routing in Mobile Ad Hoc Networks" IET Information Security , 2010, pp. 1-22.

[4] Sun, Y., Yu, W. ,Han, Z.,and Liu, K.J.R.:'Information Theoretic Framework of Trust Modeling and Evaluation for AdHoc Networks', IEEE Journal on Selected Areas in Communications, 2006, 24, (2),pp. 305-317

[5] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[6] M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "TSR: Trust-based Secure MANET Routing using HMMs," Proc. 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Vancouver, British Columbia, Canada, 27-28 Oct. 2008, pp. 83-90.

[7] Sivakumar, K.A.; Ramkumar, M., "An Efficient Secure Route Discovery Protocol for DSR," Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE , vol., no., pp.458,463, 26-30 Nov. 2007

[8] V. Balakrishnnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and Recommendations in Mobile Ad Hoc Networks," Int'l Conf. on Networking and Services, Athens, Greece, 19-25 June 2007, pp. 64-69.

[9] Pirzada, A. A., Datta, A. and McDonald, C. 2004. Trustbased routing for ad-hoc wireless networks. In Proceeding of. IEEE International Conference Networks (Singapore, 2004). 326-330.

[10] Pissinou, N., Ghosh, T. and Makki, K. 2004. Collaborative trust-based secure routing in multihop ad hoc networks. Networking (Athens, Greece 2004). Lecture Notes in Computer Science, vol. 3042, 1446-1451.

[11] Poonam, Garg, K., and Misra, M. 2010. Trust based multi path DSR protocol. In Proceedings of Fifth International Conference on Availability, Reliability and Security, (Poland, February, 2010). 204-209.