A Review of 'MANET's Security Aspects and Challenges'

Pradeep Rai
Asst. Prof., CSE Department,
Kanpur Institute of Technology,
Kanpur-208001(India)

Shubha Singh
Asst. Prof., MCA Department,
Kanpur Institute of Technology,
Kanpur -208001(India)

ABSTRACT

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aidof any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. In this thesis, we identifythe existent security threats an ad hoc network faces. To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions. In our study, we have found that necessity of secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks such as wormhole, rushing attack etc. However, inshort, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

Keywords

MANET, Security Aspects, watchdog, IDS, Clusters, Agents, PathRater

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

2. SECURITY THREATS

The wireless Channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanism scan be deployed so the boundary that separates the inside network from the outside world becomes blurred.

2.1. The existing ADHOC routing protocols such as ADHOC on Demand distance vector (**ADDV**), Dynamic Source Routing (**DSR**), Wireless MAC protocols such as (**802.11)** do not provide a trusted environment so a malicious attacker can readily become a router and disrupt network operations by disobeying the protocol specifications.

2.2. The attacker may advertise a route with a smaller distance metric than the actual distance to the destination.

2.3. By attacking routing protocol the attacker can attract traffic towards certain destination in the nodes under their control and cause the packet to be forwarded along a route that is not optional

2.4. The attacker can create routing loops in the network and introduce severe network congestion and channel contention in certain areas.

2.5. Many colluding attracters may even prevent a source node from finding any route to the destination and partition the Network.

2.6. The attacker may further subvert existing nodes in the network or fabricate its identity and impersonate.

2.7. A pair of attacker nodes may create a wormhole and shortcut the normal flows between each other

2.8. The attacker may target the route maintenance process and advertise that an operational link is broken.

2.9. One more problem is the attacker along an established route may drop the packet, modify the content of packet or duplicates the packets it has already forwarded.

2.10. Denial of service: Attack via network layer packet blasting ,in which the attacker injects a large amount of junk packets in to the network, these packets waste a significant portion of the network resources and introduce severe wireless channel contention and network congestion in MANET .

The wireless Channel is a band width constraints and also shared among multiple networking entities. The computational capacity of the mobile node is also a constrained. Because mobile devices have very limited energy sources. The main issue for MANET is to maintain proper security and no compromise with the network performance.

3. MANET’S SECURITY SERVICES

A MANET is a network consisting of a collection of nodes capable of communicating with each other without help from infrastructure of the network. There are mainly five security services:

3.1. Authentication

Correct identity is known to the communicating partner.

3.2. Confidentiality

Message information is kept secure from unauthorized party.

3.3. Integrity

Message is unaltered during communication.

3.4. Non Repudiation

The origin of the message cannot deny having sent the message.

3.5. Availability

The normal service provision in face of all kind of attacks.

Security means the security mechanism for all protocols involved in this (MANET) service to protect the basic function of MANET means security during bit transfer from one node to another.

4. LAYERS INVOLVES IN MANET APPLICATION LAYER

Detecting and preventing virus, worms, malicious codes, application abuses.

Transport Layer:-Authentication and securing end-to end communications through data encryption.

Link Layer:-Protecting the wireless MAC protocol and providing link layer security support.

Physical Layer: Providing signal jamming denial of service attacks.

5. SECURITY: “SECURITY MEANS SECURE WEAKEST LINK”

Fundamental challenge in security design for MANET is to maintain network performance with full security strength, because when more security features are introduced in the network Increases computation, communication and management overhead .this can affect the network performance. Security involves two approaches:

A. Proactive:-This approach attempt to thwart security threats in the first place through various cryptographic techniques.

B.Reactive: First detect the threat react accordingly. Due to the absence of a clear line of defence, a complete security solution for MANET should involve both approaches.

So the way to check the security is **Prevention, Detection** and **Reaction**.

Try to increase the difficulties for the attacker to penetrate the system but intrusion free system is not feasible, so the detection component play a important role to detect the attacker so that proper action can be taken to avoid persistent adverse effects.

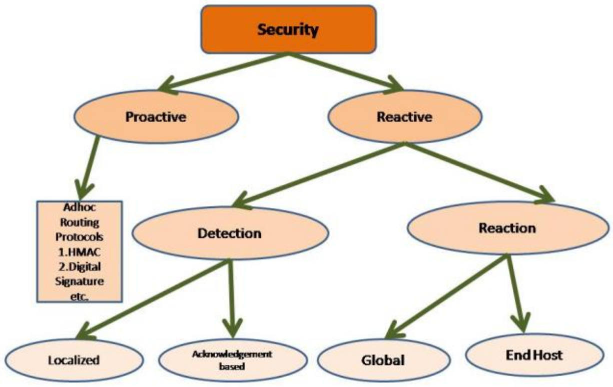
Prevention can be achieve by secure Adhoc routing protocols that prevent the attackers form installing incorrect routing states at other nodes .These protocols employ different cryptographic primitives

A.HMAC (Massage authentication codes)

B.Digital Signature

C. Hash Chain

Because the wireless channel is open, each node can perform localized detection by overhearing ongoing transmission and evaluating the behaviour of its neighbours but its accuracy is limited by a no. of factors such as channel error, interference and mobility. A malicious node may also abuse the security solutions and intentionally accuse legitimate nodes, In order to address such issues, the detection results at individual nodes can be integrated and refined in a distributed manner to achieve consensus among a group of nodes. An alternative approach relies on explicit acknowledgement from the destination and/or intermediate nodes to the source so that the source can figure out where the packet was dropped. Once a malicious node is detected certain actions are triggered to protect the network from future attacks launched by this node the reaction component is related to the prevention component in the security system. Once multiple nodes in a local neighbourhood have reached consensus that one of their neighbours is malicious, they collectively revoke the certificate of the malicious node. The malicious node is isolated in the network as it cannot participate in the routing or packet forwarding operations in the future. The pathrater allows each node to maintain its own rating for every other node it knows about .A node slowly increases the rating of well behaved nodes overtime, but dramatically decreases the rating of a malicious node that is detected by its watchdog. Based on rating source always selects the path with the highest average rating.



Security Approaches Used in MANET

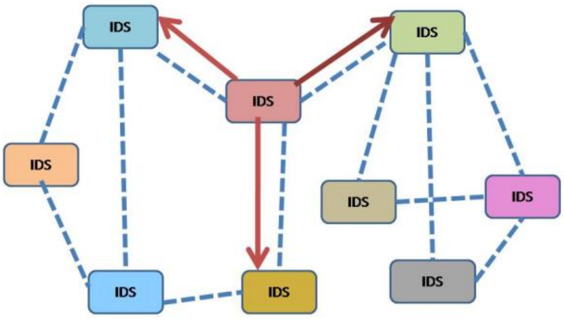
Figure 1

6. SECURITY SCHMES IMPLEMENTED IN THE MOBILE AD HOC NETWORKS

There are many different schemes which are used to secure the Mobile ad hoc network. Some of these are discussed below:

6. 1. INTRUSION DETECTION TECHNIQUES IN MANET

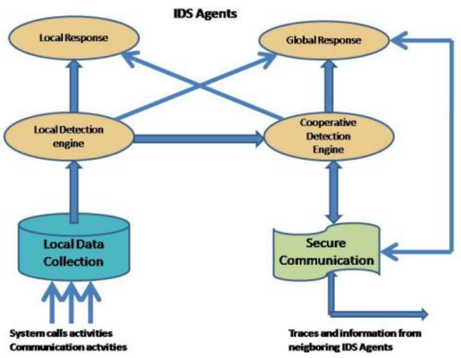
Intrusion detection is not a new concept in the network research. Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems the proposed architecture of the intrusion detection system



An IDS Architecture for Manet

Figure 2

In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behaviour locally and independently, which are performed by the built-in IDS agent. However, the neighbouring nodes can share their investigation results with each other and cooperate in a broader range. The cooperation between nodes generally happens when a certain node detects an anomaly but does not have enough evidence to figure out what kind of intrusion it belongs to. In this Situation, the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the intruder. The internal structure of an IDS agent is shown in following figure



A conceptual Model for an IDS Agent

Figure 3

In the conceptual model, there are four main functional modules:

6.1.1. Local data collection module

This mainly deals with the data gathering issue, in which the real-time audit data may come from various resources.

6.1.2..Local detection engine

Which examines the local data collected by the local data collection module and inspects if there is any anomaly shown in the data? Because there are always new attack types emerging as the known attacks being recognized by the IDS, the detection engine should not expect to merely perform pattern recognition between known attack behaviours and the anomalies that are likely to be some intrusions: instead of the misuse detection technique that cannot deal with the novel attack types effectively, the detection engine should mainly rely on the statistical anomaly detection techniques, which distinguish anomalies from normal behaviours based on the deviation between the current observation data and the normal profiles of the system.

6.1.3..Cooperative detection engine

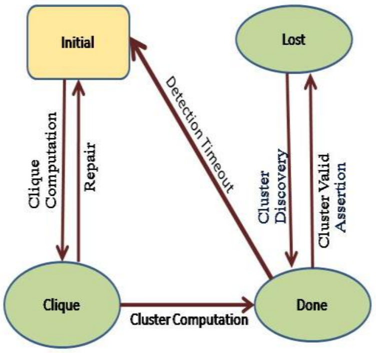
Which works with other IDS agents when there are some needs to find more evidences for some suspicious anomalies detected in some certain nodes? When there is a need to initiate such cooperated detection process, the participants will propagate the intrusion detection state information of themselves to all of their neighbouring nodes, and all of the participants can calculate the new intrusion detection state of them based on all such information they have got from their neighbours by some selected algorithms such as a distributed consensus algorithm with weight. Since we can make such a reasonable assumption that majority of the nodes in the ad hoc network should be benign, we can trust the conclusion drawn by any of the participants that the network is under attack.

6.1.4. Intrusion response module

This deals with the response to the intrusion when it has been confirmed. The response can be reinitializing the communication channel such as reassigning the key, or reorganizing the network and removing all the compromised nodes. The response to the intrusion behaviour varies with the different kinds of intrusion

6. 2.CLUSTER-BASED INTRUSION DETECTION TECHNIQUE FOR AD HOC NETWORKS

We have discussed cooperative intrusion detection architecture for the ad hoc networks in the previous part, which was first presented by Zhang et al. However, all of the nodes in this framework are supposed to participate in the cooperative intrusion detection activities when there is such a necessity, which cause huge power consumption for all the participating nodes. Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and not cooperative with other nodes so as to save their battery power, which will actually violate the original intention of this cooperative intrusion detection architecture. To solve this problem a cluster-based intrusion detection technique is used in this technique A MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue in a certain period of time, which is generally called **clusterhead**. A cluster is a group of nodes that reside within the same radio range with each other, which means that when a node is selected as the clusterhead, all of the other nodes in this cluster should be within 1-hop vicinity. It is necessary to ensure the fairness and efficiency of the cluster selection process. Here fairness contains two levels of meanings: the probability of every node in the cluster to be selected as the clusterhead should be equal, and each node should act as the cluster node for the same amount of time. Efficiency of the process means that there should be some methods that can select a node from the cluster periodically with high efficiency. The finite state machine of the cluster formation protocol is shown in Figure



Finite State Machine of the Cluster Formation Protocol

Figure 4

Basically there are four states in the cluster formation protocol: initial, clique, done and lost. All the nodes in the network will be in the initial state at first, which means that they will monitor their own traffic and detect intrusion behaviours independently. There are two steps that we need to finish before we get the cluster head of the network: clique computation and clusterhead computation. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link. The definition of clique is a little more restricted than that of cluster. Once the protocol is finished, every node is aware of its fellow clique members. Then a node will be randomly selected from the clique to act as the clusterhead. There are two other protocols that assist the cluster doing some validation and recovery issues, which are respectively called Cluster Valid Assertion Protocol and Cluster Recovery Protocol. The cluster valid assertion protocol has generally been used in the following two situations:

1. The node in the cluster will periodically use the Cluster Valid Assertion Protocol to check if the connection between the clusterhead and itself is maintained or not. If not, this node will check to see if it belongs to another cluster, and if it also get negative answer, then the node will enter the LOST state and initiate a routing recovery request.

2. Furthermore, there need to be a mandatory re-election timeout for the clusterhead to keep the fairness and security of the whole cluster. If the timeout expires, all the nodes switch from DONE state to INITIAL state and begin a new round of clusterhead election.

The Cluster Recovery Protocol is mainly used in the case that a citizen loses its connection with previous clusterhead or a clusterhead loses all its citizens, when it enters LOST state and initiates Cluster Recovery Protocol to re-discover a new clusterhead.

6. 3. MISBEHAVIOUR DETECTION THROUGH CROSS-LAYER ANALYSIS

Some *smart* attackers may simultaneously exploit several vulnerabilities at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehaviour detector. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehaviour detector. Nevertheless, this attack scenario can be detected by a cross-layer misbehaviour detector, in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way. First of all it will be an important problem that how to make the cross-layer detection more efficient, or in other words, how to cooperate between single-layer detectors to make them work well. Because different single-layer detectors deal with different types of attacks, there can be some different viewpoints to the same attack scenario when it is observed in different layers. Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers. Second, we need to find out how much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single-layer detector. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account and compared with the performance gain caused by the use of cross-layer detection method.

7. CONCLUSION

We try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention. We start with the discussion on the security criteria in mobile ad hoc network, which acts as a guidance to the security-related research works in this area. Then we talk about the main attack types that threaten the current mobile ad hoc networks. In the end, we discuss several security techniques that can help protect the mobile ad hoc networks from external and internal security threats. During the survey, we also find some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved

8. ACKNOWLEDGMENTS

The authors would like to express their cordial thanks to Mr. **Anshul Pandey** (Research Engineer Intel, USA) and Mr. **Chandresh Verma** (Project Manager, Satyam) for their valuable advice.

9. REFERENCES

[1] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in *Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, Fairfax, Virginia, 2003, pp. 135 – 147.

[2] Data Integrity, from *Wikipedia, the free encyclopedia*,http://en.wikipedia.org/wiki/Data_integrity.

[3] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, San Antonio, TX, January 2002.

[4] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in *Proceedings of ACM MOBICOM'02,* 2002.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in *Proceedings of ICNP'02,* 2002.

[6] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, *Ad Hoc Networks,* 1 (1): 175–192, July 2003.

[7] Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in *Proceedings of IEEE INFOCOM'03*, 2003.

[8] C.Tseng, P.Balasubramanyam,C. Ko, R.Limprasittiporn, J.Rowe, and K.Levitt, "A Specification-based Intrusion Detection System for AODV", in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks(SASN03)*, Fairfax, VA, USA, pp. 125–134, 2003.

[9] Y.Huang and W.Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN03),* Fairfax, VA, USA, pp. 135-147, 2003.

[10] M.Kefayati, H.R.Rabiee, S. G.Miremadi, and A.Khonsari, "Misbehavior Resilient Multi-path Data Transmission in Mobile Ad-hoc Networks", in *Proceedings of the FourthACM Workshop on Security of Ad Hoc and Sensor Networks (SASN06)* Alexandria, VA, USA, pp. 91-100, 2006.

[11] Y.Xue and K.Nahrstedt, "Providing Fault-Tolerant Ad hoc Routing Service in Adversarial Environments", *Wireless Personal Communication,* vol. 29, issue 3-4, pp. 367-388, 2004.

[12] L.Anderegg and S.Eidenbenz, "Ad hoc-VCG: A Truthful and Cost-efficient Routing Protocol for Mobile Ad Hoc Networks with Selfish Agents", in *Proceedings of the 9th*

[13] *Annual international Conference on Mobile Computing and Networking (MOBICOM03),* San Diego, CA, USA, pp. 245-259, 2003. Glomosim 2.03,http://pcl.cs.ucla.edu/projects/glomosim/.

[14] J. Parker, A. Patwardhan and A. Joshi, "Cross-layer Analysis for Detecting Wireless Misbehavior", in *Proceedings of the IEEE Consumer ommunications and NetworkingConference*(*CCNC 2006*), Las Vegas, Nevada, USA, Jan. 2006.