Analysis and Diminution of Security Attacks on Mobile Ad hoc Network

K.P.Manikandan
HOD/MCA
Chirala Engineering College
Chirala, A.P.

Dr.R.Satyaprasad
CPBS
Achariya Nagarjuna University
Nagarjuna Nager

Dr.Rajasekhararao
PRINCIPAL
KL University
Vadeshwaram

ABSTRACT

A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructure less, multi-hop network. The wireless and distributed nature of MANETs poses a great challenge to system security designers. The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: firstly, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; secondly, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; thirdly, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; The work mainly focuses on identifying preventive methods of impersonation security attacks on MANET.

1. INTRODUCTION

Ad-hoc is "For a particular purpose (improvised, made up in an instant)" or "spontaneous network", is especially useful when dealing with wireless devices in which some of the devices are part of the network only for the duration of a communications session and the need for a dynamic network topology is eminent. Many proposed routing protocols for ad hoc networks operate in an on-demand fashion, as on-demand routing protocols have been shown to often have lower overhead and faster reaction time than other types of routing based on periodic (proactive) mechanisms. Significant attention recently has been devoted to developing secure routing protocols for ad hoc networks, including a number of secure on demand routing protocols that defend against a variety of possible attacks on network routing. For example, Dynamic Source Routing (DSR), Ad hoc On demand Distance Vector (AODV), etc. There are different routing attacks, such as flooding, black hole, link spoofing, wormhole, and colluding mis-relay attacks. The existing security solutions of wire networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks.

Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource constrained in MANET. They still not perfect in terms of tradeoffs between effectiveness and efficiency. Some solutions work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol. However, the proposed research work will overcome limitations of MANET routing problems, and to resource constraints. The work will deal with security issues in mobile ad hoc networks. It will lead on to designing security architecture in tackling security challenges mobile ad hoc networks are facing.

This paper is discussed the present security architecture in a layered view and analyzes the reasoning for such security architecture. This security architecture can be used as a frame work when designing system security for ad hoc networks. A key element to the proposed framework is that it will combine well-known cryptographic mechanisms (such as digital certificates and signatures), with different sources of identification information. This information comes in the form of attributes

describing physical node characteristics, much like the biometrical characteristics examined during human identification and authentication.

2. ROUTING ATTACKS AND COUNTER MEASURES IN MANET

The venomous routing nodes can attacks in MANET using dissimilar ways, so that, the following subsections are discussed various issues of routing attacks and its countermeasures to mitigating security attacks on MANET.

2.1. Route Disruption Attack (Flooding Attack)

This type of attack attempts to disrupt MANET routing processes by sending manipulated routing messages that include source and/or destination nodes that do not exist in the MANET. Distribution of routing messages referring to non-existent nodes not only increases network load but nodes may also add non-existent routes to their routing tables.

Two variants of this attack are possible in AODV: one sends RREQ messages with a fake target node, the other sending RREP messages with forged sender node. The first step to achieve a successful attack using this method is to create a node ID not yet listed in the routing table of the attacker (which does however not guarantee that such a node does not exist in the network). In the first variant the attacker generates a RREQ message with a created node ID as target node and sends it with a TTL value set to maximum. In the second variant the attacker generates a RREP message with an existing node as destination but with a fake ID as sender ID. Additionally sequence numbers of messages are incremented before they are sent.

A simple mechanism proposed to prevent the flooding attack in the AODV protocol [11]. In this approach, each node monitors and calculates the rate of its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake. In [3], the authors show that a flooding attack can decrease throughput by 84 percent. The authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets.

Similar to [11], in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in [11], where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

2.2. Wormhole Attack

Wormhole attacks [1] use two cooperating network nodes to re-route data traffic. In order for this to be successful the two nodes must "ally" themselves and establish an additional channel outside normal network communications serving as a tunnel. Wormhole attacks are named as such as they mimic this hypothetical physical phenomenon. In this type of attack the two nodes mask that they are not directly adjacent nodes, instead they pretend to be neighbors and therefore dispose fast connections to each other and their neighbors. As these paths are used for sending data that is not part of the proper network wormholes are very difficult to detect.

Wormholes themselves are not necessarily only negative for a network as such a shortcut can have positive benefits such as relief for network traffic or shorter transfer times for packets on routes containing the wormhole. Attackers use wormholes in the network to make their nodes appear more attractive (with perceived faster transfer times) so that more data is routed through their nodes.

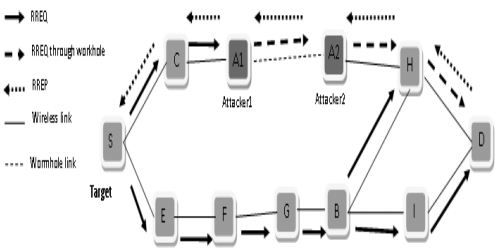

Figure 1: Wormhole attack on reactive routing

Figure 1 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked.

During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors C and E forward the RREQ as usual. However, node A1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its colluding partner A2. Then, node A2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a high speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-H-D that indeed passed through A1 and A2 to send its data.

In [6], packet leashes are proposed to detect and defend against the wormhole attack. In particular, the authors proposed two types of leashes: temporal leashes and geographical leashes. For the temporal leash approach, each node computes the packet expiration time, *te*, based on the speed of light *c* and includes the expiration time, *te*, in its packet to prevent the packet from traveling further than a specific distance, *L*. The receiver of the packet checks whether or not the packet expires by comparing its current time and the *te* in the packet. The authors also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks. For the geographical leash, each node must know its own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. Therefore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization needs not to be highly tight.

In [10], the authors offer protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of a public key infrastructure and time-stamp synchronization between all nodes that is similar to the geographic leashes proposed in [6]. In this approach, a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum transmission range, the node judges that the HELLO message is highly suspicious and might be tunneled by a wormhole attack. In [9], the authors propose a statistical analysis of multipath (SAM), which is

an approach to detect the wormhole attack by using multipath routing. This approach determines the attack by calculating the relative frequency of each ink that appears in all of the obtained routes from one route discovery. In this solution, a link that has the highest relative frequency is identified as the wormhole link. The advantage of this approach is that it introduces limited overhead when applied in multipath routing. However, it might not work in a non-multipath routing protocol, such as a pure AODV protocol.

2.3. Blackhole Attacks

Complete refusal to participate in a network, can be sudden. MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network.

Attacks in the network layer have generally two purposes: not forwarding the packets or adding and

changing some parameters of routing messages; such as sequence number and hop count. A basic attack that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place. In blackhole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all objects; data packets [7].

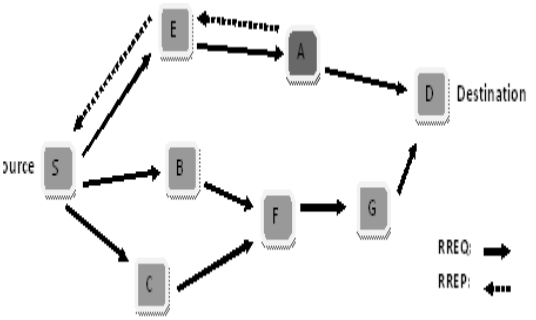

Figure 2: Blackhole attack on AODV

Figure 2 shows an example of a blackhole 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 nodes' sequence numbers, the source node S will choose the route that passes through node A.

The route confirmation request (CREQ) and route confirmation reply (CREP) is introduced in [8] to avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the blackhole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path. In [2], the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main draw back of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive. In another attempt [5], the authors analyzed the blackhole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the blackhole attack, based on differences between the destination sequence numbers of the received RREPs. The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection.

2.4. Colluding misrelay attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as *watchdog* and *pathrater* [8]. Figure 3 shows an example of this attack.

Consider the case where node A1 forwards routing packets for node T. In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In [4] the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

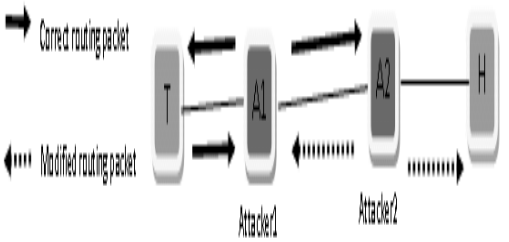

Figure 3: Colluding misrealy attack

A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the network require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient. In [9], the author proposes a method to detect an attack in which multiple malicious nodes attempt to drop packets by requiring each node to tune their transmission power when they forward packets. As an example, the author studies the case where two colluding attackers drop packets. The proposed solution requires each node to increase its transmission power twice to detect such an attack. However, this approach might not detect the attack in which three colluding attackers work in collusion. In general, the main draw back of this approach is that even if we require each node to increase transmission power to be K times, we still cannot detect the attack in which K + 1 attackers work in collusion to drop packets.

Therefore, further work must be done to counter against this type of attack efficiently.

3 SOLUTIONS TO THE RELATED WORKS

3.1. Outlier Detection

Palpanas et al. propose a model-based outlier detection algorithm in sensor networks. In their algorithm, normal behaviors are first characterized by predictive models, and then outliers can be detected as the deviations. Subramaniam et al. propose an online outlier detection mechanism for sensor networks. In this mechanism, every sensor node will keep a sliding window of the historic data and approximate the data distribution to detect the outliers. In a recent paper by Sheng et al., a histogram-based outlier detection algorithm is studied, and sensor data distribution is estimated by the histogram-based method. This method can reduce communication cost under two different detection schemes.

Moreover, a histogram refinement technique for some crucial portion of data distribution has been applied to obtain more information about outliers. Branch et al. propose an in-network outlier detection scheme to detect the outliers based on data exchange among neighbors. In this scheme, all the sensor nodes will first calculate the local outlier(s). Then some messages, which contain the local outlier(s) as well as some other supportive information, will be exchanged among all the nodes.

The message exchanging process will not halt until all the nodes have the same global view of outlier(s). Our proposed outlier detection algorithm is somewhat similar to the method proposed by Branch et al. However, there are two significant differences between the two methods. First, the method by Branch et al. does not consider the mobility of the nodes, whereas our proposed method takes the mobility issue in consideration. Second, there is no malicious behaviors in the discussion of the method by Branch et al., i.e., the nodes will not deliberately fabricate fake local views or alter incoming local views in their method. On the contrary, we have considered the malicious behaviors of the nodes, and applied the knowledge of trust and reputation as the countermeasure to the malicious behaviors.

3.2 Gossip-based Outlier Detection Algorithm

The goal of the algorithm is to find the top *k* outliers in terms of some observed behaviors such as packet drops or misroutes) from all the nodes in mobile ad hoc networks (Here *k* is a user-defined parameter). The algorithm leads to a coincident global view of the top *k* outliers in all the nodes as long as these nodes do not change their behavior significantly during the convergence time of the algorithm. By using constrained gossiping, the algorithm avoids flooding the network.

3.2.1. Algorithm Description

The proposed outlier detection algorithm contains the following four steps, namely local view formation, local view exchange, local view update, and global view formation. We have adopted two local view update methods in our algorithm: one is the simple averaging method, in which all the local views are merged by simply averaging them; the other method is the trust-based weighted method, in which the local views are merged incorporating the trust in other nodes.

The first step of our algorithm is the formation of local views. The nodes monitor and record the possible malicious behaviors of other nodes within their radio range. Each node generates its local view of outliers based on their own observations. Once all the nodes form their local views, they will broadcast the local views to all of their immediate neighbors, i.e., all the nodes that are one hop away from them.

CONCLUSION

Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both proactive and reactive approaches. Moreover, the wireless channel is accessible to both legitimate users and malicious attackers. The boundary that separate the inside network from the outside world becomes blurred. *Device with weak protection:* portable devices, as well as the system security information they store, are vulnerable to compromises. In this paper, we have discussed current routing attacks and countermeasures against MANET protocols. Some solutions that rely on cryptography such as collaborative outlier detection algorithm for securing mobile ad hoc networks and the gossip-based outlier detection algorithm can help us identify the outliers, which are generally the nodes that have exhibited some kind of abnormal behaviors. Given the fact that benign nodes rarely behave abnormally, it is highly likely that the outliers are malicious nodes. However, the solution should comprise of all three components: prevention, detection and reaction.

REFERENCES

[1] W. Wang and B. Bhargava, "Visualization of Wormholes in Sensor Networks," in *Proceedings of the 2004ACMWorkshop.*

[2] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.

[3] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[4] B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks,"IEEE GLOBECOM'06.

[5] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.

[6] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC,vol. 24, no. 2, Feb. 2006.

[7] Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, AtılımUniversity,September2006.

[8] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th MobiCom, Boston, MA,Aug.2000.

[9] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," IEEE Wireless Commun. And Networking Conf. '05.

[10] D. Raffo et al., "Securing OLSR Using Node Locations," Proc. 2005 Euro. Wireless, Nicosia,Cyprus, Apr.10–13,2005.

[11] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11,no. 2, 2005.