Authenticated Intrusion Detection in MANETs

Anu Mathews
Dept. of Computer Science & Engineering
T. John Institute of Technology, Bangalore

Dr. T. R. Mahesh
Professor & Head, Dept. of Computer Science & Engineering
T. John Institute of Technology, Bangalore

***Abstract*— A Mobile Ad hoc Network (MANET) is a collection of autonomous mobile nodes with wireless transmission capabilities without any existing infrastructure or centralized administration. In such a network, every single node works both as a transmitter and a receiver. Nodes within the same communication range directly communicate with each other; otherwise they rely on their neighbours to relay messages. The self-configuring and self-maintaining capability of a MANET makes it a much practical solution in critical military applications and also in scenarios like natural or human-induced disasters. But due to the dynamic topology, open medium and distributed environment, a MANET is highly vulnerable to different types of attacks. Security solutions used in wired networks cannot be deployed in such an environment. To protect MANET from malicious attackers, various intrusion-detection mechanisms are used. In this paper, an acknowledgement-based intrusion detection mechanism, which detects malicious nodes without much impact on network performances is being proposed.**

***Index Terms*—Mobile Ad hoc Network (MANET), Adaptive ACKnowledgement (AACK), Digital Signature, Digital Signature Algorithm (DSA).**

I. INTRODUCTION

A Mobile Ad hoc Network consists of self-configuring and self-maintaining mobile nodes which makes it possible to create a new network quickly. The nodes in a MANET are equipped with both a wireless transmitter and a receiver that communicate with each other through bidirectional wireless links either directly or indirectly. When the distance between two nodes is beyond the communication range of their own, the intermediate nodes are used to relay data transmissions. There are basically two types of networks, single-hop and multi-hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. In a multi-hop network, nodes rely on other intermediate nodes to transmit, if the destination node is out of their radio range. Unlike traditional wireless network, MANET has a decentralized network infrastructure and all the nodes are free to move randomly [8]. Minimal configuration and quick deployment make MANET useful in emergency situations where an infrastructure is unavailable or not feasible to install, such as in scenarios like natural disasters, military conflicts, medical emergency, etc.

The unique characteristics of MANET have made it very popular in the industry, especially in critical mission applications and therefore network security is of great importance. But the open medium and remote distribution of MANET make it vulnerable to different types of attacks. For example, a military base station on a battle field is a vulnerable infrastructure. Mobile Ad hoc Networks maximize total network throughput by utilising all the available nodes for routing and forwarding. But, a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. An overloaded node lacks the buffer space or available network bandwidth to forward packets. A selfish node does not spend its battery life, CPU cycles or network bandwidth to forward packets not of direct interest to it, even though it expects other nodes to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. A broken node might have a software fault that prevents it from forwarding packets.

Misbehaving nodes pose a significant problem since they degrade the average throughput. Even a few misbehaving nodes can have a severe impact. Nodes can be easily captured and compromised by malicious attackers to achieve attacks. Routing protocols in MANET assume that all the nodes in the network behave cooperatively and therefore attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Since each node is free to move around, the network topology changes continuously. Owing to the dynamic topology of MANETS, a centralized monitoring technique is not feasible in such a network. So it is essential to have an intrusion detection system in MANETs. Many research works have been done on this topic. [3], [5], [7], [10]-[13].

II. RELATED WORK

Routing protocols in MANETs assume that all the nodes in the network cooperate with each other to transmit data. Malicious attackers make use of this assumption to attack the network, by compromising few nodes. Intrusion detection systems are used to improve the security in MANETs. By detecting the attackers as soon as they enter the network, the damages caused by compromised nodes can be eliminated upfront. The three existing approaches for intrusion detection are Watchdog, TWOACK and Adaptive Acknowledgement (AACK) [6].

WATCHDOG: Marti et al. [4] proposed the Watchdog scheme which detects malicious nodes and thereby improves the network throughput. This scheme consists of two parts: Watchdog and Pathrater. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. Watchdog is implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet is removed from the buffer, since it has been forwarded on. If the packet has remained in the buffer for longer than a certain timeout, then a failure tally for the responsible node is incremented. If the tally exceeds a certain threshold bandwidth, then the node is misbehaving and a message is sent to the source to notify this misbehavior. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmissions. Watchdog is capable of detecting malicious nodes rather than links. Several intrusion detection systems have been developed as an improvement to the Watchdog scheme. But, this scheme has a number of disadvantages. It fails to detect malicious misbehaviors in the presence of the following: 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior report, 5) collusion and 6) partial dropping.

TWOACK: The six weaknesses of the Watchdog scheme were taken up for future work and new approaches were proposed to solve these issues. TWOACK proposed by Liu et al. [11] is an acknowledgement based approach that resolves the receiver collision and limited transmission power problems of Watchdog. In this scheme, every three consecutive nodes work in a group. When a node receives a packet, it has to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK works on routing protocols like Dynamic Source Routing (DSR) [2]. Fig. 1 shows the working process of TWOACK. Node A first forwards Packet 1 to node B and node B forwards it to node C. When packet 1 is received by node C, since it is two hops away from node A, it has to send a TWOACK acknowledgement packet to node A along the reverse route from node A to node C. When node A receives this TWOACK packet, then this indicates that the transmission of Packet 1 from node A to node C was successful. If the TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. This same process applies to every three consecutive nodes along the rest of the route.

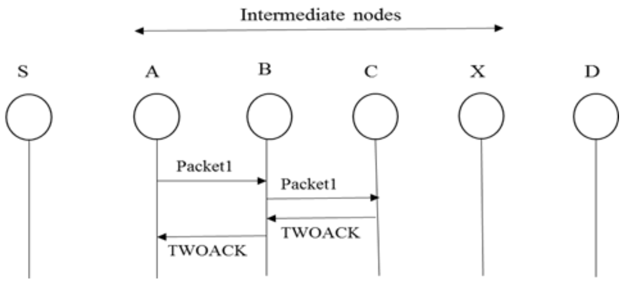

Fig.1. TWOACK scheme: Each node sends back TWOACK packet to the node that is two hops away from it.

The receiver collision and limited transmission power problems posed by Watchdog are solved in this scheme. But, a significant amount of network overhead is inevitable due to the acknowledgement process involved in every packet transmission. This may lead to degradation of the network because of the limited battery power of the devices in such a network.

AACK: Sheltami et al. proposed an acknowledgement based network layer scheme which is a combination of TWOACK and an end-to-end acknowledgement scheme called ACK. The AACK scheme reduces the network overhead significantly and also maintains the same network throughput.

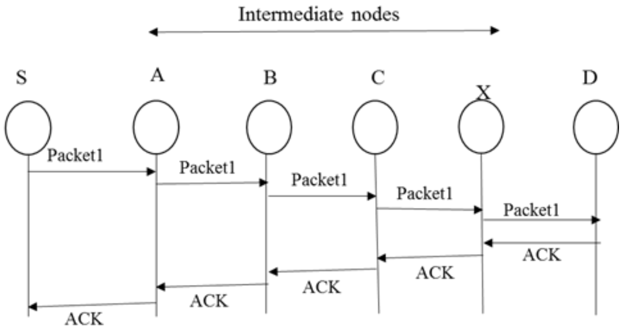

Fig.2. ACK scheme: The destination node has to send acknowledgement packets to the source node.

The end-to-end ACK process is shown in Fig.2. The working process of AACK scheme is as follows: Starting with the ACK scheme, the source node S sends out Packet 1 to the destination node D with the aid of the intermediate nodes which help in packet forwarding. When node D receives Packet 1, it has to send back an ACK acknowledgement packet to the source node S along the reverse order of the same route. The packet transmission from S to D is successful if the source node S receives this acknowledgement within a predefined time period. Otherwise the source node S will switch to a TWOACK scheme by sending out a TWOACK packet. Even though TWOACK and AACK reduce network overhead, they fail to detect malicious nodes in the presence of false misbehavior report and forged acknowledgement packets. Since the functioning of acknowledgement-based intrusion detection schemes depend on the acknowledgement packets, it is essential to guarantee the authenticity and validity of these acknowledgement packets.

Digital signature is used to ensure the authenticity, integrity and nonrepudiation of MANETs. It is an electronic analog of a written signature, which associates a message with its originating entity. First, a fixed length message digest d is computed through a pre-agreed hash function H for every message *m*. Second, the sender applies its own private key on the computed message digest to form the signature which is attached to the message *m*. The receiver can verify the signature by applying the sender's public key on the signature.

III. PROBLEM DEFINITION

The Watchdog scheme had six weaknesses .The proposed scheme, Authenticated Intrusion Detection System, overcomes three of the six weaknesses, namely, receiver collision, limited transmission power and false misbehavior report. These weaknesses are explained with typical examples in this section.

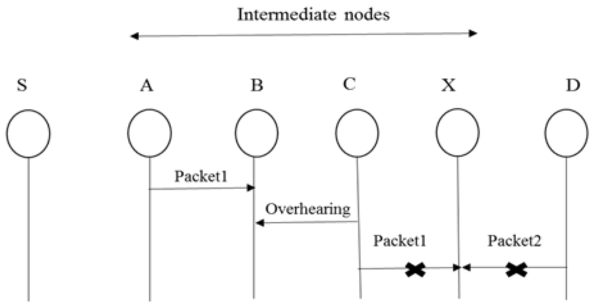

Fig. 3. Receiver collision: The nodes B and X are sending Packet 1 and Packet 2 to node C at the same time.

Receiver Collision: Fig. 3 illustrates the receiver collision problem. Node A sends Packet 1 to node B and tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such a scenario, node A overhears that node B has successfully forwarded Packet 1 to node C, but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

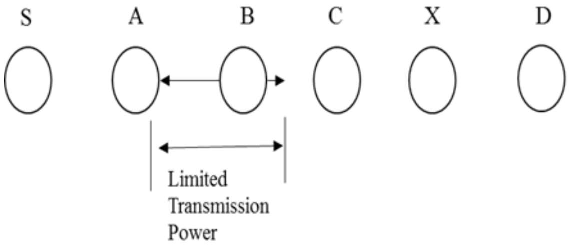

Fig. 4. Limited transmission power: Node B limits its transmission power in such a way that the packet transmission can be overheard by node A but too weak to reach node C.

Limited Transmission Power: Mobile nodes in an Ad hoc network try to limit their transmission power because of the limited battery power available to them. As shown in Fig. 4, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C.

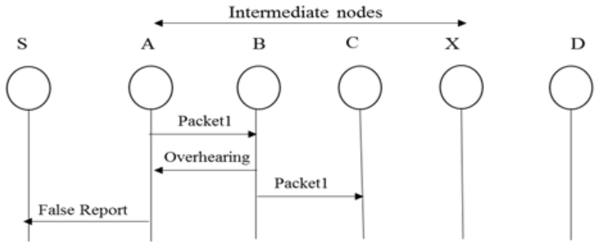

Fig. 5. False misbehavior report: Node A sends back a misbehavior report to the source node S even though node B forwarded the packet to node C.

False Misbehavior Report: A reporter node which is malicious can generate and send a false misbehavior report, so as to falsely report innocent nodes as malicious. For example, as shown in Fig. 5, node A successfully overheard that node B forwarded Packet 1 to node C, but since A is malicious, it falsely reports that node B is malicious. The TWOACK and AACK scheme solve the receiver collision and limited transmission power problems, but do not resolve the false misbehavior report problem. In this paper, an intrusion detection system which resolves receiver collision, limited transmission power problem and false misbehavior report is being proposed. A digital signature scheme, which ensures the integrity and authenticity of the acknowledgement packets is also incorporated in this approach.

IV. SCHEME DESCRIPTION

The proposed scheme is described in this section. Authenticated Intrusion Detection System for MANETs consists of three major parts: end- to- end ACK, secure ACK (S-ACK) and misbehavior report authentication (MRA). The different packet types in each of these schemes is distinguished using two bits of the six bits which are reserved in the Internet draft of DSR [2].

In the proposed scheme, the link between each node in the network is assumed to be bidirectional and also the source and destination nodes are not malicious. The authenticity and integrity of all the acknowledgement packets are ensured by digitally signing all the acknowledgement packets.

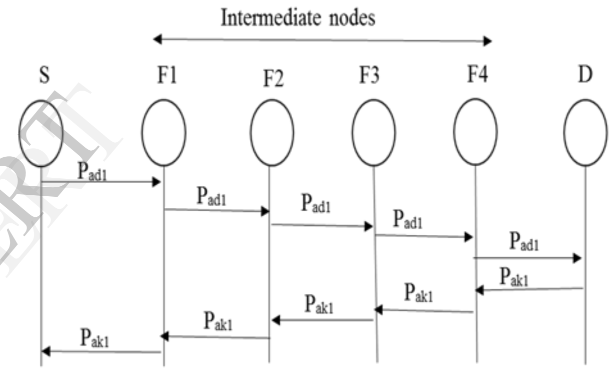

Fig. 6. ACK scheme: The destination node has to send back an acknowledgement packet to the source node when it receives a packet.

ACK

ACK is an end-to-end acknowledgement scheme. It is a part of this intrusion detection scheme which reduces the network overhead when no network misbehavior is detected. As shown in Fig. 6, in ACK mode, the source node S first sends out an ACK data packet P_{ad1} to the destination node D. If all the intermediate nodes along the route between node S and D are cooperative and node D successfully receives P_{ad1}, then node D has to send back an acknowledgement packet P_{ak1} to the source node S along the same route but in a reverse order. If the node S receives P_{ak1} within a predefined time period, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the malicious node in the route.

S-ACK

In the S-ACK scheme, which is an improved version of TWOACK [11], every three consecutive nodes work in a group

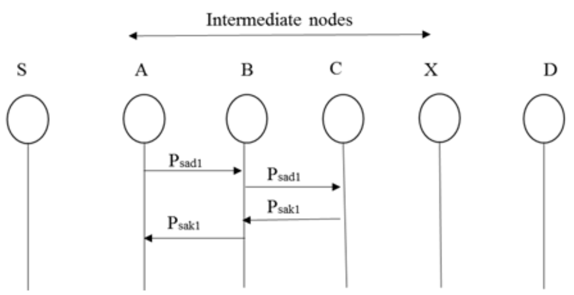

Fig. 7. S-ACK scheme: Node C is required to send back an acknowledgement packet to node A.

to detect the malicious nodes. For every three consecutive nodes along the route, the third node has to send an S-ACK acknowledgement packet to the first node in the group.

As shown in Fig. 7, the three consecutive nodes (A, B, C) work in a group to detect the misbehavior. Node A first sends out an S-ACK data packet P_{sad1} to node B, which is then forwarded to node C. When node C receives P_{sad1}, since it is the third node in the group, node C has to send back an S-ACK acknowledgement packet P_{sak1} to node B, which then forwards it to node A. If node A does not receive this acknowledgement packet within a predefined time period, both nodes B and C are reported as malicious and this misbehavior report will be sent by node A to the source node S. Instead of immediately trusting the misbehavior report, in the proposed scheme, the source node switches to MRA mode to confirm this misbehavior report.

The MRA mode is a vital step in detecting malicious misbehaviors in the presence of false misbehavior report.

MRA

A false misbehavior report is generated by malicious attackers to falsely report innocent nodes as malicious. The core of the MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

In the MRA mode, the source node first searches its local knowledge base and tries to find an alternative route to the destination node. If no other route exists, the source node starts a DSR routing request to find another route. The alternative route circumvents the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then the misbehavior report is false and the node which generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted and the nodes which were reported as malicious will be blacklisted. Hence, the MRA scheme detects malicious nodes in the presence of false misbehavior report.

Digital Signature

In the proposed intrusion detection scheme, ACK, S-ACK and MRA rely on acknowledgement packets to detect the misbehaviors in the network. Hence, the authenticity of all the acknowledgement packets needs to be ensured. All the three schemes are vulnerable if the attackers can forge the acknowledgement packets.

Digital Signature [9] is incorporated in this proposed scheme to ensure the integrity of the IDS. All the acknowledgement packets are digitally signed before they are sent out and verified until they are accepted. Digital signature in MANETs requires extra resources. So DSA and RSA digital signature schemes can be implemented to find the most optimal solution for using digital signature.

V. SIMULATION METHODOLOGIES

The simulation environment and methodology used in our proposed system is described in this section.

Scenario1: In this scenario, a basic packet dropping attack, in which malicious nodes simply drop all the packets they receive is simulated.

Scenario 2: In this scenario, malicious nodes always drop the packets that they receive and send back a false misbehavior report to the source node whenever possible.

Scenario 3: In this scenario, the attackers are smart enough to forge the acknowledgement packets.

Simulation Configurations

The proposed system will be simulated within the Network Simulator (NS) 2.35 environment on a platform with SUSE Linux 11.3.

VI. CONCLUSION

In this paper, an Intrusion Detection System has been specially designed for MANETs. The proposed system gives positive performances compared to Watchdog, TWOACK and AACK in the cases of receiver collision, limited transmission power and false misbehavior report.

Forged acknowledgement packets are avoided in this scheme by incorporating digital signatures to ensure the authenticity and integrity of the acknowledgement packets. The use of digital signatures might introduce additional routing overhead in some cases, but it can vastly improve the network performance if the attackers are smart enough to forge the acknowledgement packets. This tradeoff is worthwhile when network security is the top priority.

REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang and Tarek R Sheltami "EAACK-A Secure Intrusion Detection System for MANETs." In IEEE Transactions on Industrial Electronics, Vol.60, No. 3, March 2013.

[2] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[3] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

[5] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[6] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: SpringerVerlag, 2008.

[7] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in *Proc. Radio Wireless Conf.*, 2003, pp. 75–78.

[8] G. Jayakumar and G. Gopinath, “*Ad hoc* mobile wireless networks routing protocol—A review,” *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582, 2007.

[9] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[10] M. Zapata and N. Asokan, “Securing *ad hoc* routing protocols,” in *Proc. ACM Workshop Wireless Secur.*, 2002, pp. 1–10.

[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehaviour in MANETs,” *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[12] R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[13] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, “Secure routing and intrusion detection in ad hoc networks,” in *Proc. 3rd Int. Conf. Pervasive Comput. Commun.*, 2005, pp. 191–199.