ISSN:0975-9646

Enhance the Security Level of MANET's Using Digital Signature

M.BalaGanesh , M.Mohamed Faisal

Department of computer science and engineering, Anna University,
Sembodai Rukmani Varatharajan Engineering College, Nagapattinam, India.

***Abstract*— The routing misbehavior in MANETs (Mobile Ad Hoc Networks). In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. One such routing misbehavior is that some nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. The 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. In this paper, proposed and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.**

***Keywords*— Digital signature, DSA algorithm, EAACK, MANET.**

1. INTRODUCTION

By definition, Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

2. BACKGROUND

Intrusion Detection System (IDS):

Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system.

Some assumptions are made in order for intrusion detection systems to work. The first assumption is that user and program activities are observable. The second assumption, which is more important, is that normal and intrusive activities must have distinct behaviors, as intrusion detection must capture and analyze system activity to determine if the system is under attack.

Intrusion detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in

its analysis. Based on detection techniques, IDS can also be classified into three categories as follows.

***Anomaly detection systems*:** The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.

***Misuse detection systems*:** The system keeps patterns (or **signatures**) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.

***Specification-based detection*:** The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

3. PROBLEM DEFINITION

In this problems caused by routing misbehavior nodes and the six weaknesses of Watchdog scheme. Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme.

The Watchdog scheme fails to detect malicious misbehaviors with 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. The proposed approach EAACK is designed to tackle three out of six weaknesses.

4. PROPOSED SYSTEM

The EAACK scheme was extended with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehavior Report Authentication (MRA). In order to distinguish different packet types in different schemes, they included a two-bit packet header in EAACK. According to the Internet draft of DSR, there are six bits reserved in DSR header. In EAACK, two of the six bits were used to flag different type of packets. In the proposed scheme it was assumed that the link between each node in the network is bi-directional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.

A.ACK

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, node S first sends out an ACK data packet ad1 P to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D successfully receives ad1 P, node D is required to send back an ACK acknowledgement packet ak1 P along the same route but in a reverse order. Within a predefined time period, if node S receives ak1 P, 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 misbehaving nodes in the route.

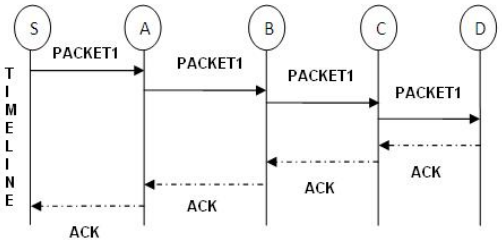

Fig 1: ACK Scheme

B. S-ACK

S-ACK scheme is an improved version of TWOACK scheme proposed by Liu et al. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

In S-ACK mode, the three consecutive nodes (i.e. F1, F2 and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet to node F2. Then node F2 forwards this packet to node F3.

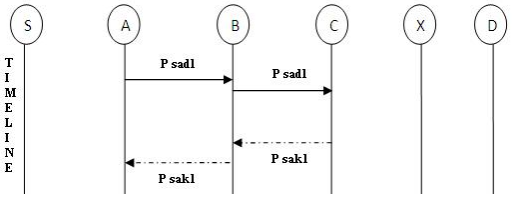

Fig 2: SACK Scheme

When node F3 receives, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. sadP sadP sakP sakP. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

C. MRA

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious.

This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

5. COMPARISON WITH OVERHEARING TECHNIQUES

Compared with the overhearing techniques, such as watchdog in [4], the 2ACK scheme solves the problems of ambiguous collisions, receiver collisions, and limited transmission power:

- **Ambiguous Collisions:** Ambiguous collisions may occur at node N1. When a well-behaved node N2 forwards the data packet towardN3, it is possible that N1 cannot overhear the transmission due to another concurrent transmission in N1's neighborhood. The 2ACK technique solves this problem by requiring N3 to send a 2ACK packet explicitly.
- **Receiver Collisions:** Receiver collisions take place in the overhearing techniques when N1 overhears the data packet being forwarded by N2, but N3 fails to receive the packet due to collisions in its neighborhood. A misbehaving N2 will not retransmit the data packet, which costs extra energy. Again, the 2ACK technique overcomes this problem due to the explicit 2ACK packets.
- **Limited Transmission Power:** A misbehaving N2 may its transmission power such that N1 can overhear its transmission but N3 cannot. This problem is similar to the Receiver Collisions problem. It becomes a threat only when the distance between N1 and N2 is less than that between N2 and N3. The 2ACK scheme is immune to limited transmission power problem.
- **Limited Overhearing Range:** A well-behaved N2 may use low transmission power to send data toward N3. Due to N1's limited overhearing range, it will not overhear the transmission successfully and will thus infer that N2 is misbehaving, causing a false alarm. Both this problem and the limited transmission power problem are caused by the potential asymmetry of communication links. The 2ACK scheme is immune to the limited overhearing range issue.

With the explicit requirement of 2ACK transmissions, the 2ACK scheme solves the above problems. Compared with overhearing techniques, the 2ACK scheme has a disadvantage of higher routing overhead. This additional routing overhead is caused by the transmission of 2ACK packets. However, we will show later that, by reducing the acknowledgment ratio, Rack, the number of 2ACK transmissions can be significantly lowered.

6. FALSE MISBEHAVIOUR REPORTS AND INTENTIONAL DROPPING OF 2ACK

A misbehaving node N1 as shown in Fig. 1 may send false misbehavior reports regarding the next-hop link, N2 →N3. However, the 2ACK scheme makes sure that such a behavior will not benefit node N1:

1) N1 may still be included in alternative routes.
2) N1 needs to forward data packets to N2 as necessary.

Otherwise, it will be detected as part of a misbehaving link (by the node preceding it on the route). A misbehaving node N3 may refuse to send any 2ACK packet for the data packets that have been received. As a result, N1 declares the link N2→N3 as misbehaving and sends a misbehavior report to the source. Since N3, as a misbehaving node, refuses to forward data packets, N2 will also declare the link of N3→ N4 (the node following N3) as misbehaving. Thus, links around node N3 are declared misbehaving and will be avoided by future route selections. Note that this might seem to have achieved the goal of slandering node N2 by N3. On the contrary, our mechanism of misbehaving link detection instead of misbehaving node detection protects node N2. The link N2→ N3 will be marked as misbehaving, but there is no accusation of N2 (or N3). Other links associated with node N2 might still be used.

Detection of the misbehaving node N3 and its punishment are trickier. Essentially, consensus needs to be developed among the majority of neighbors of node N3 to punish it. Similarly, when there are consecutive misbehaving nodes on the route, the first misbehaving node and its forwarding link will be detected and reported to the source. Such a route will be avoided in the next round of route discovery. Topology changes may also lead to false misbehavior reports. When two well-behaved neighboring nodes move out of each other's range, the link between them will fail in terms of data delivery. In 2ACK, this is taken care of by the routing scheme in use (DSR). When the sender of the link notices that the receiver is out of range, it will submit a Route Error (RERR) message to report the link failure.

7. PERFORMANCE EVALUATION

In this section, we present our simulation results for performance evaluation. Since the 2ACK scheme works as an add-on technique for the DSR protocol, the performance of the 2ACK scheme is actually the performance of the DSR+2ACK scheme.

Simulation Methodology and Performance Metrics: In the simulations, we used a version of Network Simulator (NS-2) that includes wireless extensions developed by the CMU Monarch project group. We modified the DSR module in NS-2 to simulate misbehaving nodes. The observation period of the 2ACK scheme was set to T_{obs} ¼ 0:8 second. Unless specified otherwise, the 2ACK scheme used R_{ack} ¼ 0:20, R_{mis} ¼ 0:85, and a timeout value of ┬¼ 0:15 second. The IEEE 802.11 MAC was used with a channel data rate of 11 Mbps. The data packet size was 512 bytes. The wireless transmission range of each node was R ¼ 250 m. In the simulations, N ¼ 50 mobile nodes were randomly distributed in a 700 m by 700 m flat area. The source and the destination nodes were randomly chosen among all nodes in the network.

The following metrics to measure the performance of the 2ACK scheme with respect to UDP traffic:

Packet Delivery Ratio, PDR: The ratio of the number of packets received at the destination and the number of packets sent by the source.

Routing Overhead, RO: The ratio of the amount of routing related transmissions (RREQ, RREP, RERR, and 2ACK) to the amount of data transmissions. The amounts are in bytes. Both forwarded and transmitted packets are counted.

Number of False Alarm, NFA: The number of false misbehavior reports. For TCP traffic flows, the packet delivery ratio as defined in the UDP traffic scenario would be similar for different schemes. This is because the TCP senders automatically detect end-to-end transmission failures. To better investigate the performance of EAACK under different types of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1: In this scenario, we simulated a basic packet dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watchdog, namely, receiver collision and limited transmission power.

Scenario 2: This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

Scenario 3: This scenario is used to test the IDSs' performances when the attackers are smart enough to forge acknowledgment packets and claiming positive result while, in fact, it is negative. As Watchdog is not an acknowledgment-based scheme, it is not eligible for this scenario setting.

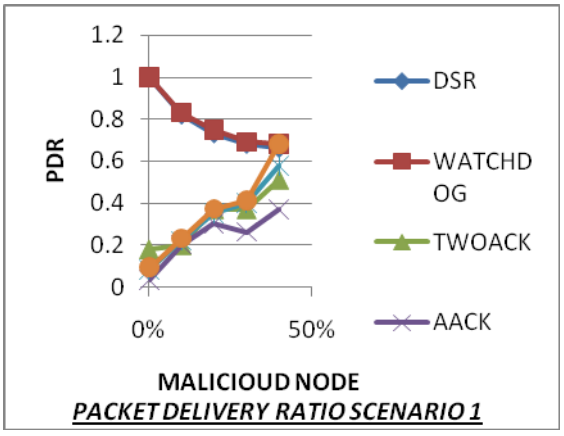

Fig. 3. Packet Delivery ratio for scenario 1

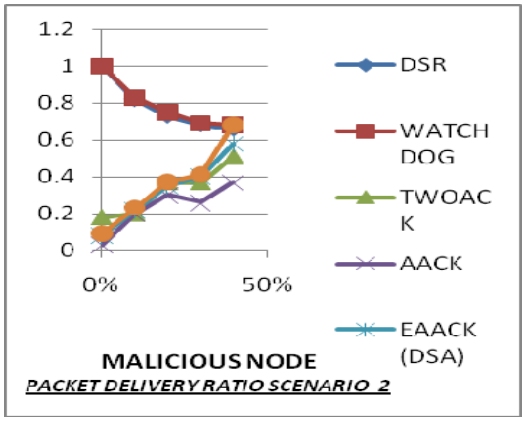

Fig. 4. Packet Delivery ratio for scenario 2

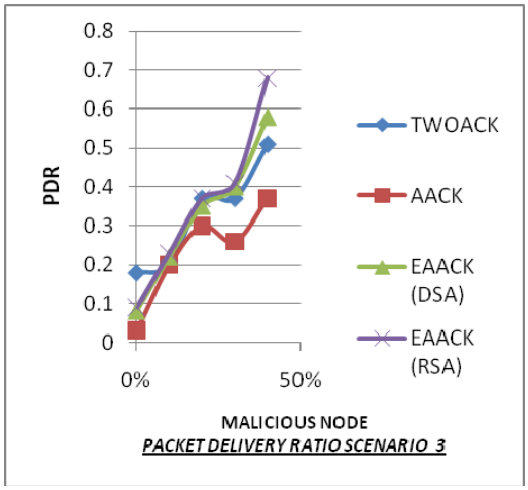

Fig. 5. Packet Delivery ratio for scenario 3.

The simulation results of RO in the above explained scenarios are shown in the above Figures. We observe that DSR and Watchdog scheme achieve the best performance, as they do not require acknowledgment scheme to detect misbehaviors. For the rest of the IDSs, AACK has the lowest overhead. This is largely due to its hybrid architecture, which significantly reduces network overhead. Although EAACK requires digital signature at all acknowledgment process, it still manages to maintain lower network overhead in most cases. We conclude that this happens as a result of the introduction of our hybrid scheme.

8. RESULT AND DISCUSSION

Wireless networking is now the medium of choice for many applications. Mobile ad hoc networks (MANETs) combine wireless communication with a high degree of node mobility. Intrusion Detection Techniques for Node Cooperation in MANET Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report.

In an effort to prevent the attackers from initiating forged data attacks extended my research work to incorporate security in my proposed scheme. Although it generates more Routing Overhead (RO) in the present scheme as demonstrated for some cases, it can vastly advance the network's Packet Delivery Ratio (PDR), when the attackers are smart enough to forge acknowledgment packets. Believe that this tradeoff is valuable when network security is the top priority. Proposed system implemented both DSA and RSA schemes in this project work. Eventually, the reason is that data transmission in MANETs consumes the most battery power. In literature survey, the DSA scheme is more suitable to be implemented in MANETs. Thus the data packets send and received with secure acknowledgement transmission.

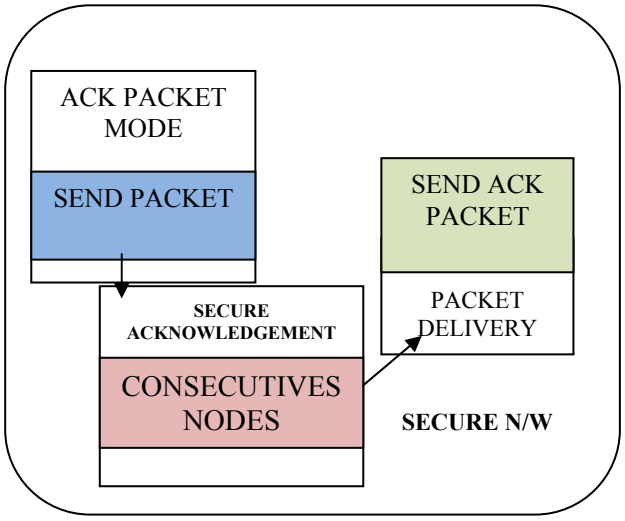

Fig 6.secure acknowledgement network

9. CONCLUSIONS AND FUTURE WORK

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme.

REFERENCES

[1] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," *IEEE Trans. Instrum.Meas.*, vol. 57, no. 7, pp. 1379–1387, Jul. 2008.

[2] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks," Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.

[3] L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Wireless Networks," http://secowinet.epfl.ch/, 2006.

[4] L.M. Feeney and M. Nilsson, "Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment," Proc. IEEE INFOCOM, 2001.

[5] L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proc. MobiHoc, Aug. 2000.

[6] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, Nov./Dec. 1999.

[7] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks," Proc. Seventh Int'l Workshop Security Protocols, 1999.

[8] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP '01), 2001.

[9] I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. MobiCom, 2004.

[10] 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.

[11] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[12] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[13] 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.