An Improved Intrusion Detection System for MANETs using Digital Signature

V.SRINIVASAN\(^1\), R.SUDHA\(^2\), G.SRINIVASAN\(^3\)

\(^1\)Professor, Dept of CSE, Annamalai University, Chidambaram, TamilNadu, India, E-mail: vsceu@gmail.com.
\(^2\)PG Scholar, Dept of CSE, Annamalai University, Chidambaram, TamilNadu, India, E-mail: sudharaj_cse@yahoo.co.in.
\(^3\)Staff I, Broadcom Ltd, Bangalore, Karnataka, India, E-mail: gsrinivasn50@gmail.com.

Abstract: In recent years Mobile Ad-Hoc Networks(MANETs) have become a very popular research topic. By providing communications in the absence of a fixed infrastructure MANETs are an attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences and the like. However, this flexibility introduces new security risks. Since prevention techniques are never enough, Intrusion Detection Systems(IDS) which monitor system activities and detect intrusions, are generally used to complement other security mechanisms. Intrusion Detection for MANET is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. Conventional IDS are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. Our work outlines issues of conventional Intrusion Detection methods like watchdog and Two Ack schemes. We propose and implement a new Intrusion-Detection System using cryptographic technique like Digital Signatures and results will demonstrate positive performances against conventional schemes in the cases of receiver collision, Limited transmission power and false misbehavior report. In this paper we propose an enhanced intrusion detection scheme by combining ACK, S-ACK, MRA and digital signature and compare it with watchdog and TWOACK.

Keywords: Digital Signature, Digital Signature Algorithm (DSA), Mobile Ad Hoc Networks (Manets), Adaptive Acknowledgement (AACK).

I. INTRODUCTION

The wide enhanced Intra spread adoption of wireless technologies has caused the computer networks concept to be re-shaped. As a consequence, new kinds of networking architectures have been developed in the last years to cope with some scenarios where the traditional wired networks are not a possible solution. Mobile ad hoc networks (MANETs) are a clear example of a new novel communications paradigm based on wireless technology and designed specifically to be used in scenarios where a fixed infrastructure is impossible to deploy. This network architecture mainly differs from other conventional wireless networks by having no fixed infrastructure. A MANET consists of mobile nodes interconnected by multi-hop communication paths where nodes themselves define the topology. Therefore, the topology of the network changes dynamically as mobile nodes join or depart from the network, or when radio links between nodes become unusable. These changes on the topology are managed by specific protocols such as AODV [2], OLSR [3] or DYMO [4], which spread the information about network changes among all nodes of the MANET. The up growth of MANETs becomes evident if we think about the specific target scenarios.

Special situations without any previous infrastructure, like emergency missions, military operations or ad hoc meetings rely on this network architecture to deploy a communications system. However, the absence of infrastructure makes MANETs more vulnerable to attacks than other conventional networks. Since the protocols designed for MANETs are based on the cooperation among nodes (and, therefore, on the confidence on these nodes), its specifications cope well with network topology changes. However, it also makes them vulnerable against malicious attacks. There are several kinds of attacks that can take place in MANETs, but in this work we will only focus solely on the attacks that are specific to the data transmission process. One of the main attacks against ad hoc networks affecting their routing protocols are named routing-disruption attacks. Such attacks can be considered as instances of a denial-of service (DoS) attack, since they compromise the routing of packets, thus affecting the availability of certain (or all) network and application services. An example of these kinds of attacks is the selfish node, which uses the network but does not cooperate, saving battery life for its own communications. Another similar attack is the black hole, which intends to disrupt the
communication with its neighborhood by attracting all traffic flows in the network and then dropping all packets received without forwarding them to their final destination.

The existence of these attacks makes the network availability quite unpredictable. Notice that network availability is a minimum requirement for developing any commercial system, and MANETs are not an exception. Therefore extra effort must be achieve an acceptable security level. In particular, trustworthiness is essential for the practical exploitation of these networks. Several techniques have been developed to avoid these kinds of attacks. Existing ad hoc security solutions can be classified into three main categories [5]: key management, secure routing, and cooperation enforcement. Key management guarantees the identification and copes with all the problems concerning keys; secure routing uses the established keys to ensure the authentication, the confidentiality and the integrity in both the topology discovery and the data forwarding phases; finally, cooperation enforcement fights selfish behaviors and encourages the cooperation between nodes.

In the scope of this work, we will focus on the last category. In this context, intrusion detection systems (IDS) aim at monitoring the activity of the nodes in the network in order to detect misbehavior. A basic module in the construction of such systems is the watchdog [6], a component used for the detection of selfish nodes and malicious attackers. When a node forwards a packet, the watchdog verifies that the next node in the path also forwards the packet. Other reputation systems, like the Pathrater [7] and Routeguard [8] solutions, isolate and/or punish misbehaving nodes or routes by decreasing their trustability rates. In this work, we test an implementation of a watchdog module and TWOACK scheme using the NS2 simulator [9]. Although watchdog seem to be a useful tool for IDS, and also the base for other related techniques, our results show that they are highly affected by node mobility, an intrinsic characteristic of MANETs. This affects the credibility of the watchdog when applied to MANETs: the higher the mobility is, the more false positives and false negatives the watchdog incurs in. Hence, in this work we make a deep study of the watchdog, TWOACK and their problems. An enhanced scheme is suggested in this paper with digital Signature.

II. BACKGROUND

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.

TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [11].

The working process of TWOACK is shown in Fig. 1 Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog.

Fig1. TWOACK Scheme

Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication[12]. The development of cryptography technique has a long and fascinating history. Process of cryptography can be generalized as a data string, which
associates a message (in digital form) with some originating entity, or an electronic analog of a written signature [13].

Digital signature schemes can be mainly divided into the following two categories.

1. Digital signature with appendix: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA) [13].

2. Digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA [14].

In this paper, we implemented both DSA and RSA in our proposed IDS scheme. The main purpose of this implementation is to compare their performances in MANETs.

The general flow of data communication with digital signature is shown in Fig. 2. First, a fixed-length message digest is computed through a preagreed hash function $H$ for every message $m$. This process can be described in Eq.(1)

$$H(m)=d.$$  

(1)

Second, the sender Alice needs to apply its own private key $P_{r-sender}$ on the computed message digest $d$. The result is a signature $S_{r-sender}$, which is attached to message $m$ and Alice’s secret private key given in Eq.(2)

$$S_{pr-sender}(d)=\text{Sig}_{sender}.$$  

(2)

To ensure the validity of the digital signature, the sender is obliged to always keep its private key $P_{r-sender}$ as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, sender can intercept the message and easily forge malicious messages with Alice’s signature and send them to receiver. As these malicious messages are digitally signed by sender, receiver sees them as legitimate and authentic messages from sender. Thus, Eve can readily achieve malicious attacks to receiver or even the entire network.

Next, sender can send a message $m$ along with the signature $\text{Sig}_{Alice}$ to receiver via an unsecured channel. Receiver then computes the received message $m'$ against the preagreed hash function $H$ to get the message digest $d'$. This process can be generalized as

$$H(m')=d'.$$  

(3)

Receiver can verify the signature by applying Alice’s public key $P_{r-sender}$ on $\text{Sig}_{sender}$ by using

$$S_{pk-sender}(\text{Sig}_{sender})=d.$$  

(4)

If $d==d'$, then it is safe to claim that the message $m'$ transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

Fig. 2. Communication with Digital Signature

### III. PROBLEM DEFINITION

TWOACK solves weaknesses like receiver collision and limited transmission power. However, it is vulnerable to the false misbehavior attack. In this paper, our goal is to propose new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem. Furthermore, we extend our research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets. Proposed IDS is consists of 4 components, namely, ACK, secure ACK (S-ACK), misbehavior report authentication (MRA) and Digital Signature. In order to distinguish different packet types in different schemes, we included a 2-b packet header in this scheme. According to the Internet draft of DSR [15], there is 6-b reserved in the DSR header. In our work, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table I.

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Packet Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Data</td>
<td>00</td>
</tr>
<tr>
<td>ACK</td>
<td>01</td>
</tr>
<tr>
<td>S-ACK</td>
<td>10</td>
</tr>
<tr>
<td>MRA</td>
<td>11</td>
</tr>
</tbody>
</table>

TABLE I

Packet Type Indicators

Fig. 3 presents a flowchart describing the proposed IDS scheme. Please note that, in our proposed scheme, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this paper are required to be digitally signed by its sender and verified by its receiver.
Fig. 3. System control flow

Fig. 3 shows the system flow of how our IDS scheme works.

IV. SCHEME DESCRIPTION

A. ACK

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

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liuet al.[16]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment 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. As shown in Fig. 4, 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 $P_{sad1}$ to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives $P_{sad1}$, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet $P_{sak1}$ to node F2. Node F2 forwards $P_{sak1}$ back to node F1. If node F1 does not receive this acknowledgment 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. Nevertheless, unlike the 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. This is a vital step to detect false misbehavior report in our proposed scheme.

C. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report 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. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we circumvent 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 it is safe to conclude that this is a false misbehavior report and whoever
An Improved Intrusion Detection System for MANETs using Digital Signature

generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, our proposed IDS is capable of detecting malicious nodes despite the existence of false misbehavior report.

D. Digital Signature

As discussed before, proposed IDS is an acknowledgment based IDS. All three parts namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in proposed IDS are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. With regard to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, it is required that all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, the extra overhead is improved with the introduction of digital signature in MANETs. The goal is to find the most optimal solution for using digital signature in MANETs.

V. PERFORMANCE EVALUATION

A. Simulation in NS2

To better investigate the performance of proposed IDS 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.

B. Simulation Configuration

In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670x670 m. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512. For each scheme, we ran every network scenario three times and calculated the average performance.

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics.

1. Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2. Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQUEST (RREQ), Route REPLY (RREP), Route ERROr (RERR), ACK, S-ACK, and MRA].

During the simulation, the source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

Regarding the digital signature schemes, we adopted an open source library named Botan [19]. This cryptography library is locally compiled with GCC 4.3. To compare performances between DSA and RSA schemes, we generated a 1024-b DSA key and a 1024-b RSA key for every node in the network. We assumed that both a public key and a private key are generated for each node and they were all distributed in advance. The typical sizes of public- and private-key files are 654 and 509 B with a 1024-b DSA key, respectively. On the other hand, the sizes of public- and private-key files for 1024-b RSA are 272 and 916 B, respectively. The signature file sizes for DSA and RSA are 89 and 131 B, respectively.

C. Simulation Results

In all of the three scenarios, we witness that the DSA scheme always produces slightly less network overhead than RSA does. This is easy to understand because the signature size of DSA is much smaller than the signature size of RSA.
However, it is interesting to observe that the RO differences between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produces. We assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. With respect to this result, we find DSA as a more desirable digital signature scheme in MANETs. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.

VI. CONCLUSION AND FUTURE WORK
Packet-dropping attack has always been a major threat to the security in MANETs. In this paper, we have proposed a new Intrusion Detection System 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. Although it generates more ROs in some cases, as shown in the result, it can vastly improve the network’s PDR when the attackers are smart enough to forge acknowledgment packets. We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs.

In future, further investigations have to be carried out with the following objectives,
1. Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;
2. Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys;

VII. REFERENCES