ENHANCED ADAPTIVE ACK- PROTECTED INTERRUPTION DETECTION SYSTEM USING DIGITAL SIGNATURE FOR MANET

*Dr.N.Magesh, M.E., Ph.D.**K.Krishnakarthik B.E.,
Inst. Of Road and Transport Technology, Erode-638 316

ABSTRACT—**Themigration to wireless network from wired net-work has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless net-works, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose 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.**

Index Terms—Digital signature, Digital Signature Algorithm(DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET).

I 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 [35]. 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 par-ties 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 [10], [27], [29]. 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 [19], [30].Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [14], [28]. 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 [5], attackers can easily compromise MANETs by inserting malicious or no 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. Many research efforts have been devoted to such research topic [1]–[3], [6]–[9], [15], [16],[24], [26], [29]–[31].In the next section, we mainly concentrate on discussing the background information required for understanding this research topic.

II EXISTING SYSTEM:

A.IDS in MANETs

As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [27]. Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog [17], TWOACK [15], and Adaptive ACKnowledgment (AACK) [25].

Watchdog:Marti *et al.* [17] proposed a scheme namedWatchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, 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 [15], [20], [21], [25]. Nevertheless, as pointed out by Marti *et al.* [17], 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. We discuss these weak-nesses with further detail in Section III.

TWOACK*:* With respect to the six weaknesses of theWatchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* [16] is one of the most important approaches among them. 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 prob-lems 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 desti-nation. 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.

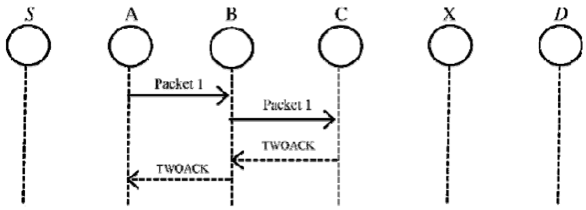


Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. 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. However, many research studies are working in energy harvesting to deal with this problem [25], [28], [29].

***AACK**:* Based on TWOACK, Sheltami *et al.* [25] pro-posed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK).

Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Fig. 2.In the ACK scheme shown in Fig. 2, the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet.

When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of thesame route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful.

Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

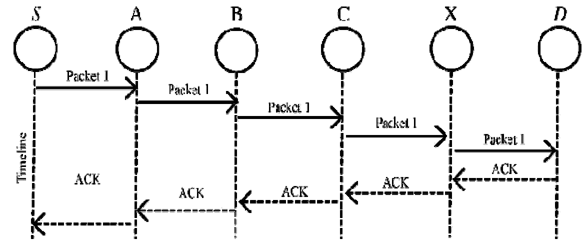


Fig. 2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

B. Digital Signature

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 [18]. Christo Ananth et al. [22] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

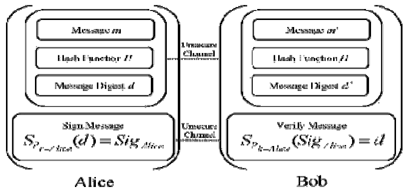


Fig. 3. Communication with digital signature.

In this research work, we implemented both DSA and RSA in our proposed EAACK 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. 3. First, a fixed-length message digest is computed through a prepared hash function H for every message m. This process can be described as

$$H(m) = d. \quad (1)$$

Second, the sender Alice needs to apply its own private key $P_{r-Alice}$on the computed message digest d. The result is asignature Sig_{Alice}, which is attached to message m and Alice's secret private key

$$S_{P_{r-Alice}}(d) = Sig_{\text{Alice}}. \quad (2)$$

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key $P_{r-Alice}$ as a se-cret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice's signature and send them to Bob. As these malicious messages are digitally signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can readily achieve malicious attacks to Bob or even the entire network.Next, Alice can send a message m along with the signature $Sig_{\text{Alice}}$to Bob via an unsecured channel. Bob then computesthe received message $\bar{m}$ against the preagreed hash function H to get the message digest $\bar{d}$. This process can be generalized as

$$H(\bar{m}) = \bar{d}. \quad (3)$$

Bob can verify the signature by applying Alice's public key $P_{k-Alice}$onSig_{Alice}, by using

$$S_{P_{k-Alice}}(Sig_{\text{Alice}}) = d. \quad (4)$$

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

III PROBLEM DEFINITION

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this section, we discuss these three weaknesses in detail.

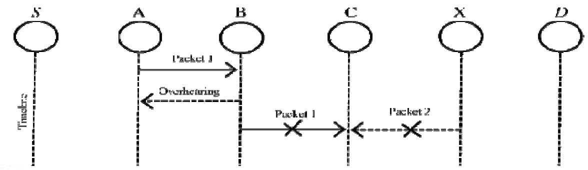


Fig. 4. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

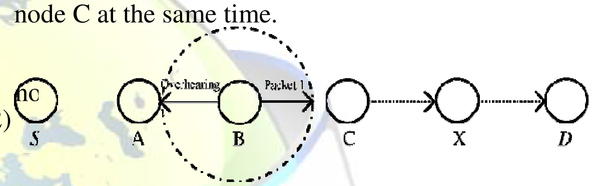


Fig. 5. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach de C.

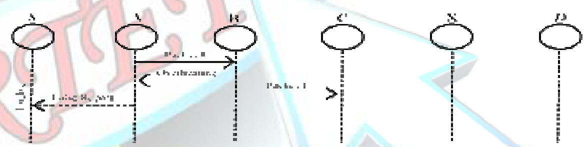


Fig. 6. False misbehavior report: Node A sends back a misbehavior report even though node B forwarded the packet to node C.

In a typical example of receiver collisions, shown in Fig. 4, after node a sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, 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. In the case of limited transmission power, in or der to pre-serve its own battery resources, 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, as shown in Fi g. 5.For false misbehavior report, although node A ccessfully overheard that node B forwarded Packet 1 to node C, node a still reported node B as misbehaving, as shown in Fig. 6. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to propose a 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 sig-nature 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.

TABLE I
PACKET TYPE INDICATORS

Packet Type	Packet Flag
General Data	00
ACK	01
S-ACK	10
MRA	11

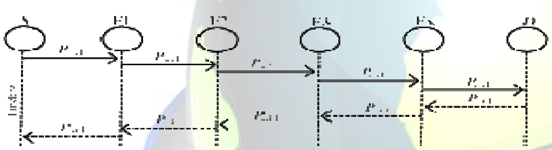


Fig. 7. System control flow: This figure shows the system flow of how the EAACK scheme works.

IV PROPOSED SYSTEM

In this section, we describe our proposed EAACK scheme in detail. The approach described in this research paper is based on our previous work [12], where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets.EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [11], there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table I.Fig. 7 (shown later) presents a flowchart describing the EAACK 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 research are required to be digitally signed by its sender and verified by its receiver.

A. ACK

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 8, in ACK mode, 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 nodes S and D are cooperative and node D successfully receives P_{ad1}, 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.

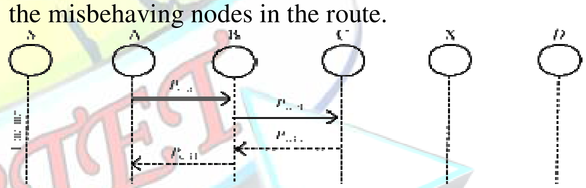


Fig. 8. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et 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. 9, 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 generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

D. Digital Signature

As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, 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 EAACK are authentic and un-tainted. 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, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA [33] and RSA [23] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

V PERFORMANCE:

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes.

A. Simulation Methodologies

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.

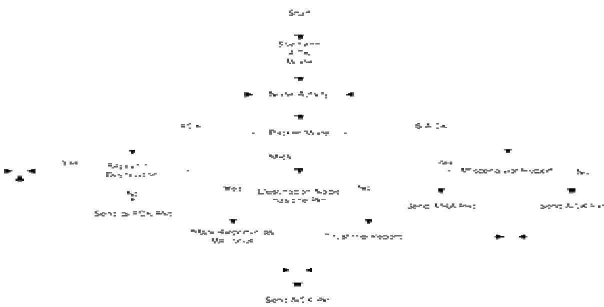


Fig. 9. S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

B. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM.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 670 × 670 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 B.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 [13].

1) ***Packet delivery ratio (PDR)*****:** PDR defines the ratio of thenumber 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 theamount 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 [32]. 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 Bwith 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.In terms of computational complexity and memory consumption, we did research on popular mobile sensors. According to our research, one of the most popular sensor nodes in the market is Tmote Sky [34]. This type of sensor is equipped with a TI MSP430F1611 8-MHz CPU and 1070 KB of memory space. We believe that this is enough for handling our simulation settings in terms of both computational power and memory space.

C. Performance Evaluation

To provide readers with a better insight on our simulation results, detailed simulation data are presented in Table II.

TABLE II

Scenario 1: Packet Delivery Ratio					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
DSR	1	0.82	0.73	0.68	0.66
Watchdog	1	0.83	0.77	0.7	0.67
TWOACK	1	0.97	0.96	0.92	0.92
AACK	1	0.96	0.96	0.93	0.92
EAACK(DSA)	1	0.96	0.97	0.93	0.91
EAACK(RSA)	1	0.96	0.97	0.92	0.92
Scenario 1: Routing Overhead					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
DSR	0.02	0.023	0.023	0.022	0.02
Watchdog	0.02	0.025	0.025	0.023	0.023
TWOACK	0.18	0.4	0.43	0.42	0.51
AACK	0.03	0.23	0.32	0.33	0.39
EAACK(DSA)	0.15	0.28	0.35	0.44	0.58
EAACK(RSA)	0.16	0.3	0.37	0.47	0.61
Scenario 2: Packet Delivery Ratio					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
DSR	1	0.82	0.73	0.68	0.66
Watchdog	1	0.83	0.75	0.69	0.68
TWOACK	1	0.93	0.84	0.82	0.79
AACK	1	0.93	0.85	0.82	0.8
EAACK(DSA)	1	0.95	0.92	0.87	0.79
EAACK(RSA)	1	0.95	0.92	0.86	0.79
Scenario 2: Routing Overhead					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
DSR	0.02	0.023	0.023	0.022	0.02
Watchdog	0.02	0.025	0.025	0.023	0.023
TWOACK	0.18	0.2	0.38	0.4	0.52
AACK	0.18	0.19	0.24	0.22	0.51
EAACK(DSA)	0.22	0.25	0.33	0.32	0.64
EAACK(RSA)	0.23	0.265	0.35	0.34	0.68
Scenario 3: Packet Delivery Ratio					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
TWOACK	1	0.91	0.79	0.65	0.61
AACK	1	0.91	0.79	0.64	0.62
EAACK(DSA)	1	0.95	0.84	0.75	0.75
EAACK(RSA)	1	0.95	0.85	0.75	0.75
Scenario 3: Routing Overhead					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
TWOACK	0.18	0.2	0.37	0.37	0.51
AACK	0.03	0.2	0.3	0.26	0.37
EAACK(DSA)	0.08	0.22	0.35	0.4	0.58
EAACK(RSa)	0.09	0.23	0.37	0.41	0.68

*1) **Simulation Results—Scenario 1:***In scenario 1, maliciousnodes drop all the packets that pass through it. Fig. 10 shows the simulation results that are based on PDR.

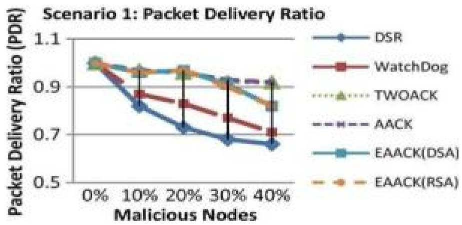
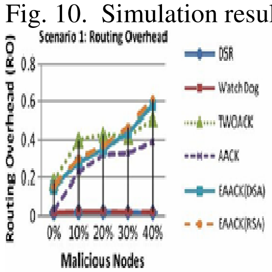


Fig. 10. Simulation results for scenario 1—PDR.



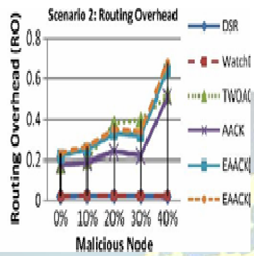


Fig. 11. Simulation results for scenario 1—RO.
Fig. 13. Simulation results for scenario 2—RO.

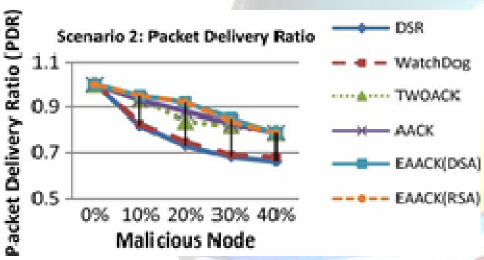


Fig. 12. Simulation results for scenario 2—PDR.

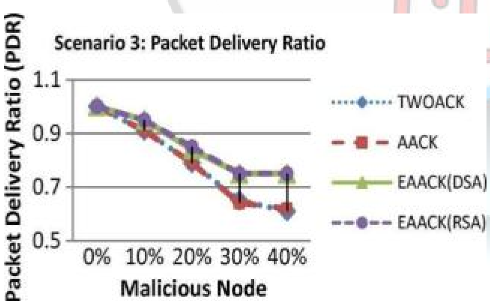


FIG 14: Simulation results for scenario 3—PDR

In Fig. 10, we observe that all acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme EAACK surpassed Watchdog's performance by 21%when there are 20% of malicious nodes in the network. From the results, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to detect misbehaviors with the presence of receiver collision and limited transmission power. However, when the number of malicious nodes reaches 40%, our proposed scheme EAACK's performance is lower than those of TWOACK and AACK. We generalize it as a result of the introduction of MRA scheme, when it takes too long to receive an MRA acknowledgment from the destination node that the waiting time exceeds the predefined threshold.

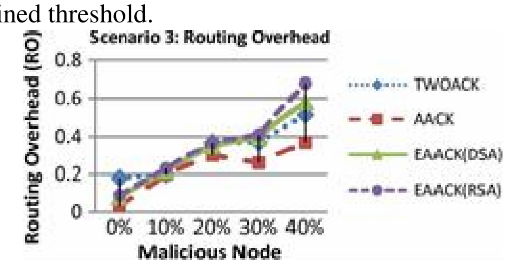


Fig. 15. Simulation results for scenario 3—RO

The simulation results of RO in scenario 1 are shown in Fig. 11. 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.

*2) **Simulation Results—Scenario 2:***In the second scenario,we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. This scenario setting is designed to test the IDS's performance under the false misbehavior report. Fig. 12 shows the achieved simulation results based on PDR. When malicious nodes are 10%, EAACK performs 2% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%, EAACK outperforms all the other schemes and maintains the PDR to over 90%. We believe that the introduction of MRA scheme mainly contributes to this performance. EAACK is the only scheme that is capable of detecting false misbehavior report.In terms of RO, owing to the hybrid scheme, EAACK maintains a lower network overhead compared to TWOACK in most cases, as shown in Fig. 13. However, RO rises rapidly with the increase of malicious nodes. It is due to the fact that moremalicious nodes require a lot more acknowledgment packets and digital signatures.

*3) **Simulation Results—Scenario 3:***In scenario 3, we pro-vide the malicious nodes the ability to forge acknowledgment packets. This way, malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to its previous node whenever necessary. This is a common method for attackers to degrade network performance while still maintaining its reputation. The PDR performance comparison in scenario 3 is shown in Fig. 14. We can observe that our proposed scheme EAACK outperforms TWOACK and AACK in all test scenarios.We believe that this is because EAACK is the only scheme which is capable of detecting forged acknowledgment packets. Fig. 15 shows the achieved RO performance results for each IDS in scenario 3. Regardless of different digital signature schemes adopted in EAACK, it produces more network over-head than AACK and TWOACK when malicious nodes are more than 10%. We conclude that the reason is that digital signature scheme brings in more overhead than the other two schemes.

DSA and RSA:In all of the three scenarios, we witnessthat 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 differentnumbers 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

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 de-signed 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. Al-though it generates more ROs in some cases, as demonstrated in our experiment, 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.To increase the merits of our research work, we plan to investigate the following issues in our future research:

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 predistributed keys;
3) testing the performance of EAACK in real network envi-ronment instead of software simulation.

REFERENCE

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, ―Which wireless technology for industrial wireless sensor networks? The development of OCARI technol,‖ *IEEE Trans. Ind. Elec-tron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

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

[3] 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.

[4] T. Anantvalee and J. Wu, ―A Survey on Intrusion Detection in Mobile Ad Hoc Networks,‖ in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, *Security and Cooperation in WirelessNetworks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, ―Model-ing and optimization of a solar energy harvester system

for self-powered wireless sensor networks,‖ *IEEE Trans. Ind. Electron.*, vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, ―Industrial wireless sensor networks: Challenges, design principles, and technical approach,‖ *IEEE Trans. Ind.Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, ―SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,‖ in *Proc. 4th IEEE WorkshopMobile Comput. Syst. Appl.*, 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, ―ARIADNE: A secure on-demand rout-ing protocol for ad hoc networks,‖ in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, ―*Ad hoc* mobile wireless networks rout-ing protocol—A review,‖ *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582, 2007.

[11] 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.

[12] 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.

[13] N. Kang, E. Shakshuki, and T. Sheltami, ―Detecting forged acknowl-edgements in MANETs,‖ in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, ―Mobile *ad-hoc*commu-nications in AEC industry,‖ *J. Inf. Technol. Const.*, vol. 9, pp. 313–323, 2004.

[15] J.-S. Lee, ―A Petri net design of command filters for semiautonomous mobile sensor networks,‖ *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

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

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ―Mitigating routing misbe-haviour in mobile ad hoc networks,‖ in *Proc. 6th Annu. Int. Conf. MobileComput. Netw.*, Boston, MA, 2000, pp. 255–265.

[18] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of AppliedCryptography*. Boca Raton, FL: CRC, 1996, T-37.

[19] N. Nasser and Y. Chen, ―Enhanced intrusion detection systems for dis-covering malicious nodes in mobile ad hoc network,‖ in *Proc. IEEE Int.Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[20] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, ―On intrusion detection and response for mobile ad hoc networks,‖ in *Proc. IEEE Int. Conf.Perform., Comput.,Commun.*, 2004, pp. 747–752.

[21] A. Patcha and A. Mishra, ―Collaborative security architecture for black hole attack prevention in mobile ad hoc networks,‖ in *Proc. Radio Wire-less Conf.*, 2003, pp. 75–78.

[22] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[23] 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.

[24] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, ―Energy harvesting from piezoelectric materials fully integrated in footwear,‖ *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 813–819, Mar. 2010.

[25] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, ―Video transmission enhancement in presence of misbehaving nodes in MANETs,‖ *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[26] A. Singh, M. Maheshwari, and N. Kumar, ―Security and trust management in MANET,‖ in *Communications in Computer and Information Science*, vol. 147. New York: Springer-Verlag,

2011, pt. 3, pp. 384–387.

[27] B. Sun, –Intrusion detection in mobile ad hoc networks,‖ Ph.D. disserta-tion, Texas A&M Univ., College Station, TX, 2004.

[28] K. Stanoevska-Slabeva and M. Heitmann, –Impact of mobile ad-hoc net-works on the mobile value system,‖ in *Proc. 2nd Conf. m-Bus.*, Vienna, Austria, Jun. 2003.

[29] A. Tabesh and L. G. Frechette, –A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator,‖ *IEEETrans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.

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

[31] L. Zhou and Z. Haas, –Securing ad-hoc networks,‖ *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.