IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

EAACK – A Secure Intrusion – Detection System for MANETs

G. Sathyanarayani[1], Dr. S. Adaekalavan[2]

Research Scholar, Department of Computer Science, JJ College of Arts and Science, Pudukkottai, India [1]

Assistant Professor, Department of Computer Applications, JJ College of Arts and Science, Pudukkottai, India [2]

Abstract: The migration to wireless network from wired network 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 networks, 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.

Keywords: Digital signature algorithm (DSA), Enhanced Adaptive Acknowledgement (EAACK), Mobile Adhoc NETwork (MANET).

I. INTRODUCTION

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired", an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them. Some history of networking is included, as well as an introduction to TCP/IP and internetworking. We go on to consider risk management, network threats, firewalls, and more special-purpose secure networking devices. This is not intended to be a ``frequently asked questions" reference, nor is it a ``hands-on" document describing how to accomplish specific functionality. It is hoped that the reader will have a wider perspective on security in general, and better understand how to reduce and manage risk personally, at home, and in the workplace.

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we'll cover some of the foundations of computer networking, then move on to an overview of some popular networks. Following that, we'll take a more in-depth look at TCP/IP, the network protocol suite that is used to run the Internet and many intranets. Once we've covered this, we'll go back and discuss some of the threats that managers and administrators of computer networks need to confront, and then some tools that can be used to reduce the exposure to the risks of network computing. A ``network" has been defined as ``any set of interlinking lines resembling a net, a network of roads an interconnected system, a network of alliances." This definition suits our purpose well: a computer network is simply a system of interconnected computers. How they're connected is irrelevant, and as we'll soon see, there are a number of ways to do this.

II. RELATED WORK

K. Al Agha and M.-H. Bertin proposed a MANET stands for Mobile Ad Hoc Network. The Ad Hoc network that is used for mobile communication is called MANET. The MANETS are used when the user is moving. Because MANET does not depends on fixed infrastructure. Wireless networks are used to connect with different networks in MANETs. Security is more critical in wireless communication when compared to the wired communication. So the security of the MANET must be optimized to secure information while transferring.

The proposed system introduces a new intrusion-detection system named Competent Enhanced Adaptive Acknowledgment (CEAACK) for finding malicious nodes using RSA digital signature and EAACK specially designed for MANETs [1].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

R. Akbani and G. V. S. Raju present in modern technology, wireless network used for effective communication. MANET [Mobile Ad hoc Network] plays a vital role in wireless communication. From mobile ad hoc network can used to fix a random node with mobility condition. All the nodes should occur in mobility and scalability. Any node can move from one place to another place without any link failure. At the same time any code can act as a misbehaving node due to malicious attackers. This is the major drawback in Mobile ad hoc network. To overcome these issues introduced a new scheme as authenticate secure acknowledgement ASA algorithm. From these algorithm can able to find out the malicious attackers correctly from the source to destination. Also analyze the performance of the entire network using simulation parameters such as packet delivery ratio and routing overhead [2].

R. H. Akbani and S. Patel Jinwala explain that Mobile Ad-hoc NETwork (MANET) is an application of wireless network with self-configuring mobile nodes. MANET does not require any fixed infrastructure. Its development never has any threshold range. Nodes in MANET can communicate with each other if and only if all the nodes are in the same range. This wide distribution of nodes makes MANET vulnerable to various attacks, packet dropping attack or black hole attack is one of the possible attack. It is very hard to detect and prevent. To prevent from packet dropping attack, detection of misbehavior links and selfish nodes plays a vital role in MANETs. In this paper, a comprehensive investigation on detection of misbehavior links and malicious nodes is carried out [3].

T. Anantvalee and J. Wu explain the use of mobile ad hoc networks (MANETs) has been widespread in many applications, including some mission critical applications, and as such security has become one of the major concerns in MANETs. Due to some unique characteristics of MANETs, prevention methods alone are not sufficient to make them secure; therefore, detection should be added as another defense before an attacker can breach the system. In general, the intrusion detection techniques for traditional wireless networks are not well suited for MANETs. In this paper, we classify the architectures for intrusion detection systems (IDS) that have been introduced for MANETs. Current IDS's corresponding to those architectures are also reviewed and compared. We then provide some directions for future research [4].

III. PROBLEM DESCRIPTION

The natural mobility and scalability, wireless networks are always preferred since the first day of their invention. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades. 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.

A. Asymmetric Encryption Algorithms

a. RSA

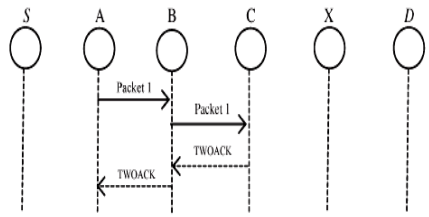
One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978 [RIVE78]. The RSA scheme has since reigned supreme as the most widely accepted and implemented approach to public-key encryption. This challenge used a public-key size (length of n) of 129 decimal digits means that larger key sizes must be used. Currently, a 1024-bit key size (about 300 decimal digits) is considered strong enough for virtually all applications.

b. Diffie-Hellman Key Agreement

The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography [DIFF76] and is generally referred to as Diffie-Hellman key exchange, or key agreement. A number of commercial products employ this key exchange technique.

B. TWOACK

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK 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 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. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).



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

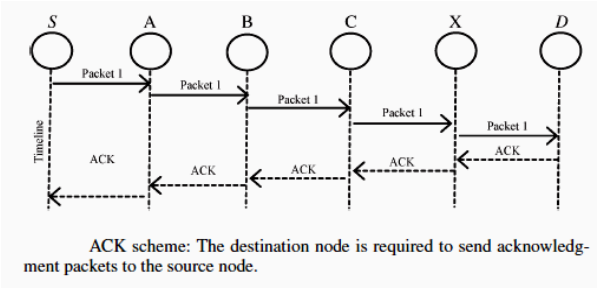
C. AACK

Based on TWOACK, 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 below in Fig.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016



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

In the ACK scheme above Fig, 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 the same 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.

D. Digital Signature

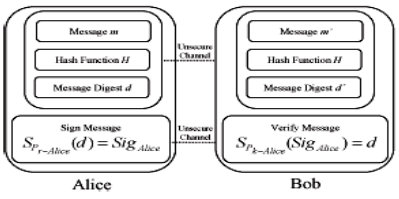
Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication . The development of cryptography technique has a long and fascinating history. The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non repudiation.

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).

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.

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



Communication with digital signature.

The general flow of data communication with digital signature is shown above fig.. First, a fixed-length message digest is computed through a preagreed hash function H for every message m. This process can be described as

$$H(m) = d$$

Second, the sender Alice needs to apply its own private keyPr−Alice on the computed message digest d. The result is a signature SigAlice, which is attached to message m and Alice's secret private key

$$SPr-Alice\ (d) = SigAlice.$$

Next, Alice can send a message m along with the signature SigAlice to Bob via an unsecured channel. Bob then computes the received messagem against the preagreed hash function H to get the message digest d. This process can be generalized as

$$H(m) = d$$

Bob can verify the signature by applying Alice's public key Pk−Alice on SigAlice, by using

$$SPk-Alice\ (SigAlice) = d.$$

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.

IV. METHODOLOGY

Mobile Ad hoc Network is a collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. A new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report and compared it against other popular mechanisms in different scenarios through simulation. The results will demonstrate positive performances against Watchdog, TWOACK and EAACK in the cases of receiver collision, limited transmission power and false misbehavior report. EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances.

- The past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically.
- The latest trend in wireless networks is towards pervasive and ubiquitous computing - catering to both nomadic and fixed users, anytime and anywhere.
- A need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

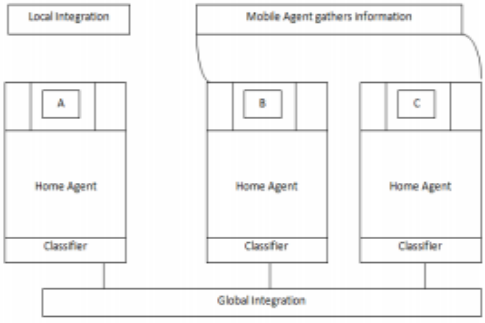
A. Problem Definition

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.

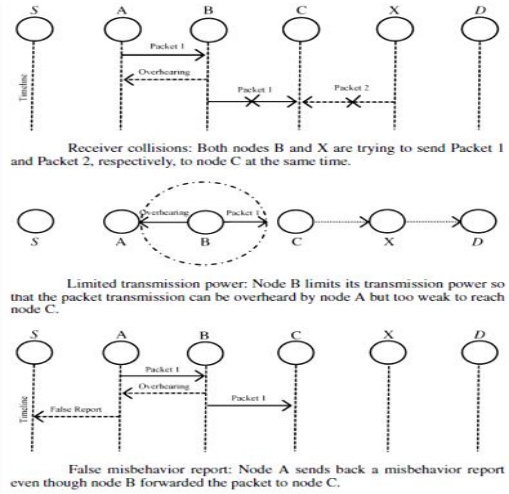
After node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C. node C.

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.

B. Flow Diagram



In the diagram represents a flow chart 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.



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

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 node C.

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

C. Digital Signature Schemes

As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, andMRA,are acknowledgment-based detect ion 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.

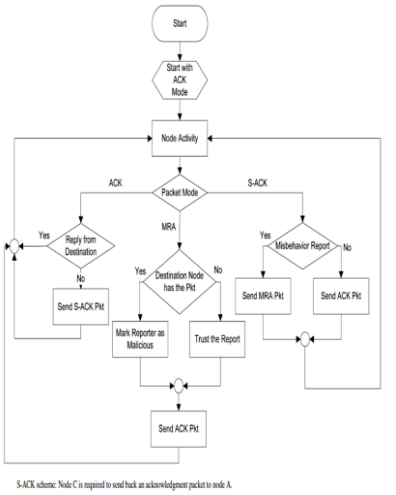
V. EXPERIMENTAL RESULTS

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.



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

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 Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu9.10. The system is running on a laptop with Core 2 Duo T7250CPU and 3-GB RAM.In order to better compare

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

our simulation results with other research works, we adopted the default scenario settings in NS2.34. The intention is to provide more general results and makeit easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of670 × 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 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 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 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. In terms of computational complexity and memory consumption, we did research on popular mobile sensors. According to our research, one of themost popular sensor nodes in themarket 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.

Table II PERFORMANCE EVALUATION

	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
Scenario 1: Packet Delivery Ratio					
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

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

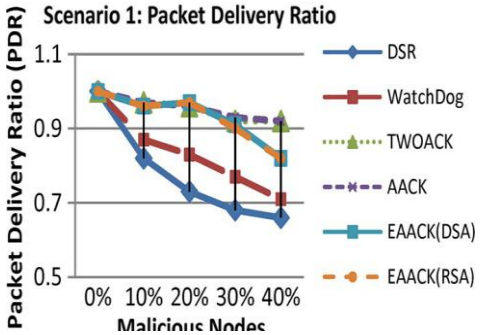


Fig. 4 Simulation results for scenario 1—PDR.

1) Simulation Results—Scenario 1:
In scenario 1, malicious nodes drop all the packets that pass through it. Fig. 4 shows the simulation results that are based on PDR. In Fig. 4, we observe that all acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme EAACK surpassed Watchdog's performance by 21%

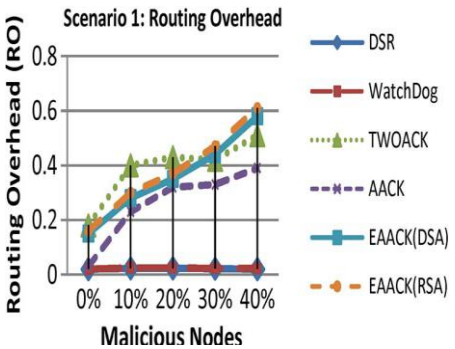


Fig. 5.Simulation results for scenario 1—RO

DOI 10.17148/IJARCCE.2016.5894

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

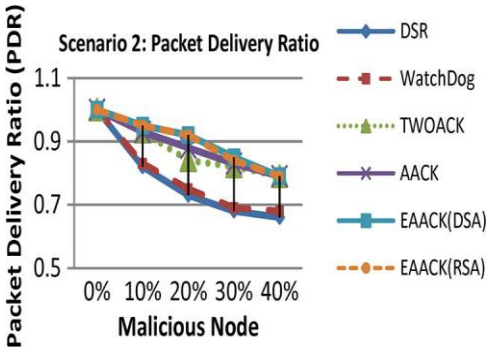


Fig. 6.Simulation results for scenario 2—PDR

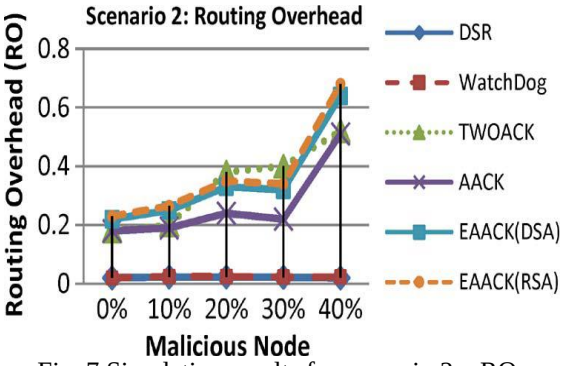


Fig. 7 Simulation results for scenario 2—RO.

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.

The simulation results of RO in scenario 1 are shown in Fig. 5. 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. 6 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 utperforms 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.

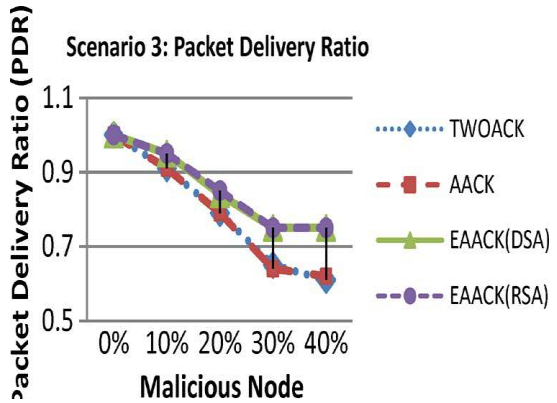


Fig. 8. Simulation results for scenario 3—PDR

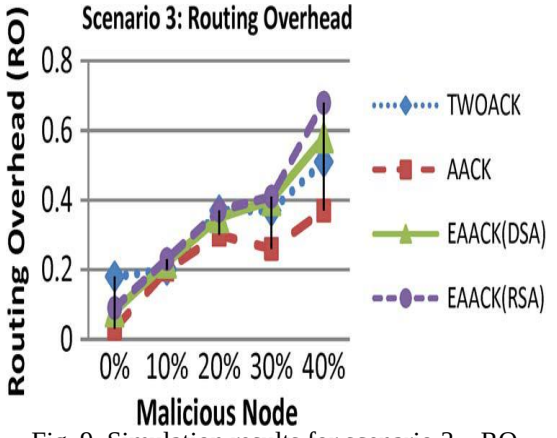


Fig. 9. Simulation results for scenario 3—RO

3) Simulation Results—Scenario 3:

In scenario 3, we provide 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. 8. 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. 9 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 overhead 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.

4) DSA and RSA:
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 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. we plan to investigate the following issues in our future research are possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature; examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of redistributed keys; testing the performance of EAACK in real network environment instead of software simulation.

REFERENCES

[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. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009
[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," inLecture 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," inProc. 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," inWireless/Mobile Security. New York: SpringerVerlag, 2008.
[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered.
[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," inProc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.
[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," inProc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.
[10] G. Jayakumar and G. Gopinath, "Ad hocmobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.
[11] D. Johnson and D. Maltz, "Dynamic Source Routing inad hocwireless networks," inMobile 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] J. Jeon, V. Lavrenko, and R. Manmatha. Automatic image annotation and retrieval using cross-media relevance models. In SIGIR, pages 119–126, 2003.
[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. 4,1835–1841, 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, 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. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.
[18] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.