A Recent Secure Intrusion Detection System for MANETS

Bindhu Madhavi.P[1] Nagendra.M[2]
[2]Head of Department
[1,2]Department of computer science engineering
[1]T.John Institute of Technology, Bengaluru-83, Karnataka [2]S.K.University Anantapur, Andhrapradesh

Abstract— As global trend changes from wired network to wireless network in the present days. This wireless network extends scalability and mobility features to serve many possible applications . Mobile Adhoc Network(MANET) is one of the critical application among all contemporary wireless networks. Compare to other traditional network, MANET does not have any fixed network infrastructure; every node in mobile network works as both transmitter and receiver. Intermediate nodes must communicates with each other, if only having same communication range. Otherwise, they relay messages onto the their neighbors. In MANET network each node having self configuring ability, that made it popular among critical mission applications. MANET vulnerable to malicious attackers due to its an open medium network and wide distribution of nodes. In this case, it is crucial to present secure intrusion-detection mechanisms to protect MANET from such attacks. In this paper, we propose and implement a new secure intrusion-detection system designed for MANETs. Compared to contemporary network approaches, it demonstrates higher malicious-behavior-detection rates in certain circumstances using DSA.

Key words: Digital signature, digital signature algorithm(DSA),Enhanced Adaptive ACKnowledgment (AACK) (EAACK),Mobile Ad hoc NETwork (MANET).

I. INTRODUCTION

Wireless networks are their having natural mobility and scalability 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. Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days.

One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. 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.

Intrusion detection is very important aspect of defending the cyber infrastructure from attackers or hackers. Intrusion prevention technique such as filtering router policies and firewalls fail to stop such kind of attacks. Therefore, no matter how well a system is protected, intrusion still occurs and so they should be detected. Intrusion detection systems are becoming significant part of security and the computer system. An intrusion detection system is used to detect many types of malicious behaviors of nodes that can compromise the security and trust of a computer system. To address this problem, IDS should be added to enhance the security level of MANETs. If

MANET knows how to detect the attackers as soon as they enter the network, we will be able to completely remove the potential damages caused by compromised nodes at the first time. IDSs are a great complement to existing proactive approaches and they usually act as the second layer in MANETs. There is a need for IDS to implement an intelligent control mechanism in order to monitor and recognize security breach attempts efficiently over a period of the expected network lifetime. The present research mechanism has focused on designing Intrusion Detection Systems (IDS) to monitor and analyze system events for detecting network resource misuse in a MANET.

II. LITERATURE SURVEY

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 (IDSs), which monitor system activities and detect intrusions, are generally used to complement other security mechanisms. Intrusion detection for MANETs 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 IDSs are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. Wireless networking is now the medium of choice for many applications. In addition, modern manufacturing techniques allow increasingly sophisticated functionality to reside in devices that are ever smaller, and so increasingly mobile. Mobile ad hoc networks (MANETs) combine wireless

communication with a high degree of node mobility. Limited range wireless communication and high node mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met. The dynamic nature of the protocols that enable MANET operation means they are readily suited to deployment in extreme or volatile circumstances.

III. Scheme Description

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

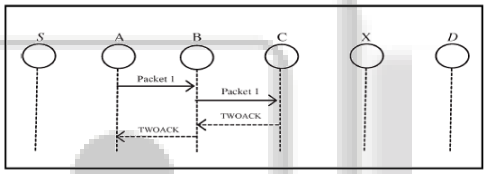

Fig. 1: TWOACK scheme

A. ACK:

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 acknowl-edgment 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 schemein ACK is shown in Fig. 2.

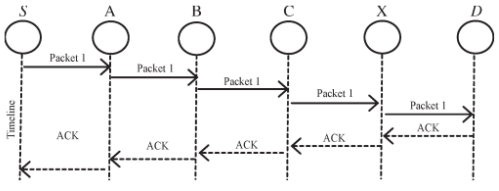

Fig. 2: ACK scheme

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 the SHAKSHUKI et al.: EAACK—A SECURE INTRUSION-DETECTION SYSTEM FOR MANETs 1091Fig. 2. ACK scheme: The destination node is required to send acknowledg-ment packets to the source node. 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. 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.

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 cryp-tography 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]. The development of cryptography technique has a long and fascinating history. The pursuit of secure communication has been conducted by human being since 4000 years ago in Egypt, according to Kahn's book [30] in 1963. Such development dramatically accelerated since the World War II, which some believe is largely due to the globalization process.

The security in MANETs is defined as a combination of pro-cesses, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and nonrepudiation [18]. Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs. It 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 [33]. 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) [33].
(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 [23].

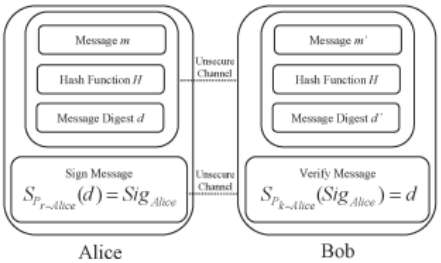

Fig. 3: Communication with digital signature

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 signa-ture is shown in Fig. 3. 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. (1)

Second, the sender Alice needs to apply its own private key Pr −Al ice on the computed message digest d . The result is a signature Sig Alice , which is attached to message m and Alice's secret private key S Pr – Alice(d)= SigAlice . (2)

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key Pr −Al ice 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 SigAlice to Bob via an unsecured channel. Bob 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) Bob can verify the signature by applying Alice's public key P k −Al ice on SigAlice ,by using S Pk – Alice (SigAlice)= d. (4) If d == d, then it is safe to claim that the message mtransmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

II. SYSTEM ANALYSIS

A. *Existing System:*

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi-hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi-hop 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.

B. *Proposed System:*

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. The false misbehaviour 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. The source route broadcasts an RREQ message to all the neighbours within its communication range. Upon receiving this RREQ message, each neighbour appends their addresses to the message and broadcasts this new message to their neighbours. 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.

III. SYSTEM DESIGN & IMPLEMENTATION

A. *Design:*

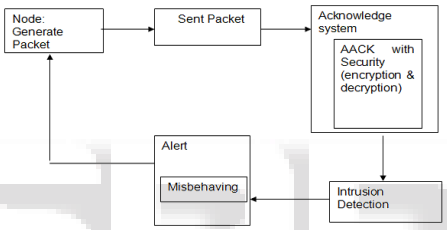

Fig. 4. Architecture Design

The above diagram shows IIDS uses AODV routing protocol to find the shortest path in the network to reach destination. Then it encrypts the data packet with hash key and send to the destination. The destination decrypts the data and check the hash value for data integrity. If the route has attacker nodes and if the sender does not receive acknowledgement packets then the packets will be sent in the new route. If any node wants to send packet to neighboring node then first source node generate the packet and send to the neighboring node. The sent packet is sent to acknowledge system in which we AACK with security. After that it send packet according to mode and detect the intruder in the system, If intruder or misbehaving node is detected then alert will be triggered by the same node that detect the misbehaving node. When a node detect malicious node it will inform the source node by sending an acknowledgement, which is a small packet that is generated by the routing protocol and extract the route from source route of corresponding data packet and the packet will be sent in a new route.

B. *Implementation:*

As discussed before, IIDS is an acknowledgment-based IDS. AACK is an acknowledgment-based detection scheme. It relies on acknowledgment packets to sense misbehaviors in the network. Thus, it is extremely important to make sure that all acknowledgment packets in IIDS are untainted and authentic. Otherwise, if the attackers are smart enough

to forge acknowledgment packets, all of the three schemes will be defenseless. With regard to this serious concern, we incorporated security in our proposed scheme. In order to make sure the integrity of the IDS, IIDS requires AACK acknowledgment packets to be encrypted before they are sent out and verified until they are accepted. In order to reduce the extra resources required due to the implementation of digital signature in MANETs, CEASAR encryption and decryption scheme has been incorporated in the present work since the ultimate goal is to find the most advantageous solution for using security in MANETs.

C. Simulation Results:

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.

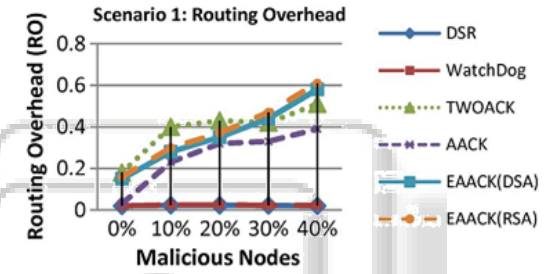

Fig. 5: Simulation results for scenario 1—RO

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.

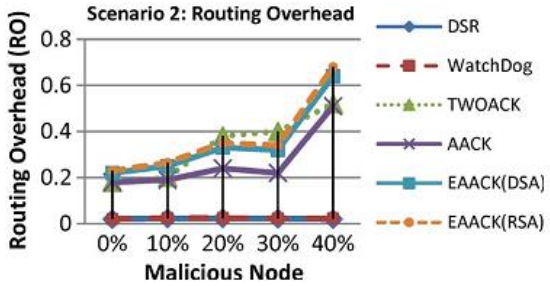

Fig.6: Simulation results for scenario 2—RO

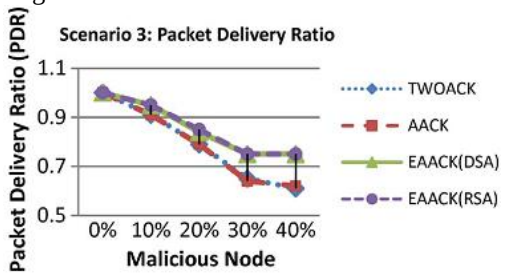

Fig.7: Simulation results for scenario 3—PDR

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.

Vi. Conclusion and Future Enhancement

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a new secure IDS 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 pre-distributed keys;
(3) Testing the performance of EAACK in real network environment instead of software simulation.

IV. 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. I nd. 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 hocnetworks: 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 Coopera tion in Wireless Networks. 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. I nd. 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. 4 th IEEE Workshop Mobile Comput. S yst. 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. 8 th AC M Int. C onf. M obiCom,Atlanta, GA, 2002, pp. 12–23.
[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks rout-ing protocol—A review," J. Comput. S ci. , 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 I nt. C onf. 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. C onf. 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. C onst., vol. 9, pp. 313–323,2004.
[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. I nd. 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. M obile 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. 6 th Annu. Int. Conf. M obile Comput. N etw., Boston, MA, 2000, pp. 255–265.

