International Journal of Innovative Research in Advanced Engineering (IJIRAE)
Volume 1 Issue 1 (April 2014)

Secure Intrusion Detection for Wireless Sensor Networks

D. Raja Vigneshwar
Post Graduate Student,
M.A.M. College of Engineering, Trichy-620021
Tamil Nadu, India.
rajavigneshwar@aol.com

Karthikeyan S.S
PG Scholar,
Regional Center for Anna University,
Coimbatore
sskarthikinfo@gmail.com

Prof.M. Pandiyanathan
Dept. of Computer Science & Engineering
M.A.M. College of Engineering, Trichy-620021
Tamil Nadu, India
pandiyanathan@mmace.org

Abstract -- The migration to wireless network from wired network has been a global trend in the past few decades 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.. 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- EAACK (Enhanced Adaptive Acknowledgement), IBOOS (Identity Based Online/Offline Signature), SACK (Selective Acknowledgement), Packet dropping, Watchdog scheme.

1. INTRODUCTION

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 par-ties 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. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly .MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks.

For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Proposed approach EAACK is designed to tackle three of the weakness of watchdog scheme, false misbehavior and collision.

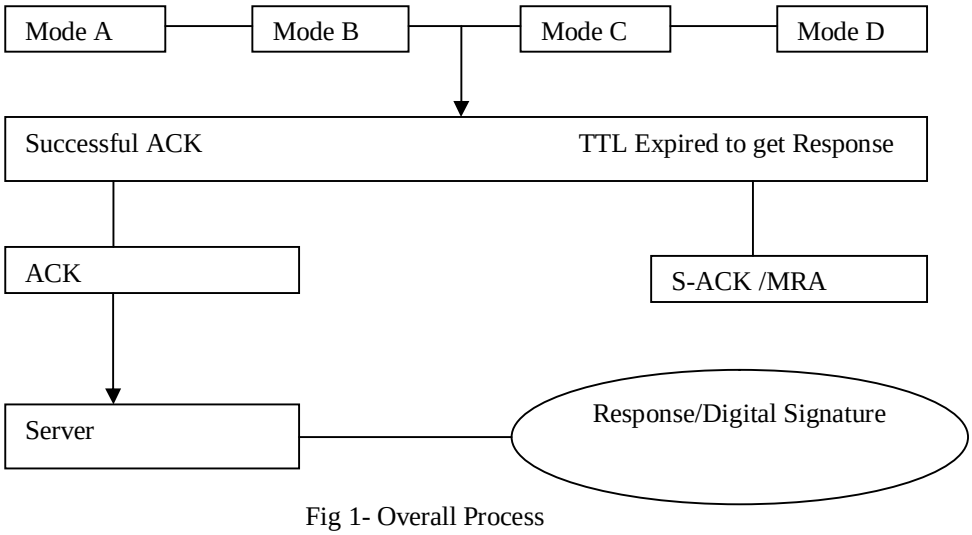

Fig 1- Overall Process

II. RELATED WORK

Watchdog detection mechanism is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link.

ACK Scheme*:* A network-layer technique to detect misbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed ACK.

End-to-end Acknowledgment Schemes: Acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks.

III. PROPOSED WORK

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 untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. 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 and RSA digital signature schemes. The goal is to find the most optimal solution for using digital signature in MANETs. Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption multiple key pairs. Having knowledge of multiple key, say the encryption key, is not sufficient enough to determine the other key - the decryption key. Therefore, the encryption key can be made public, provided the decryption key is held only by the party wishing to receive encrypted messages (hence the name public/private key cryptography). Anyone can not use the public key for others public keys and to encrypt a message, only for recipient can decrypt it. The mathematical relationship between the public/private key pair permits a general rule: any message encrypted with one key for one slot of the pair can be successfully decrypted only with that key's counterpart. To encrypt with the public key means you can decrypt only with the private key for slot by slot. The converse is also true - to encrypt with the private key means you can decrypt only with the public key.

3.1. Algorithm

EAACK is an acknowledgment-based IDS all three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes.

ACK: The hybrid scheme in EAACK to reduce network overhead when no network misbehavior is detected. ACK mode, node Source node first sends out an ACK data packet P_{ad1} to the destination node. If all the intermediate nodes along the route between Source node and Destination node are cooperative and receiver node receive the message successfully receives P_{ad1}.

S-ACK: 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.

MRA: 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

3.2. Attack Detection Techniques

The 2ACK scheme solves the problems of ambiguous collisions, receiver collisions, and limited transmission power: *End-to-end Acknowledgment Schemes:* Such acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks. The 2ACK technique differs from the ACK and the SACK schemes in the TCP protocol in the following manner: the 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive TCP, on the other hand, uses ACK and SACK to measure the usefulness of the current route and to take appropriate action. For example, congestion control is based on the reception of the ACK and the SACK packets.

4. Result Analysis

Figure 1 shows malicious node drop all the packets that pass through it. 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.

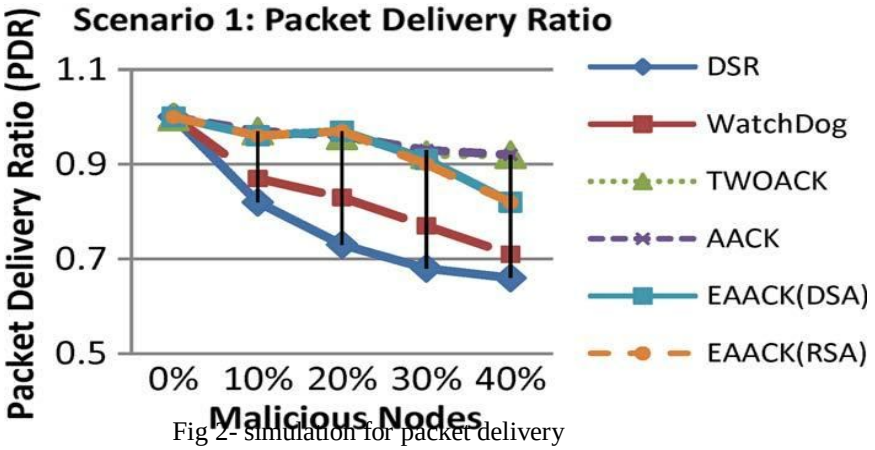

Fig 2- simulation for packet delivery

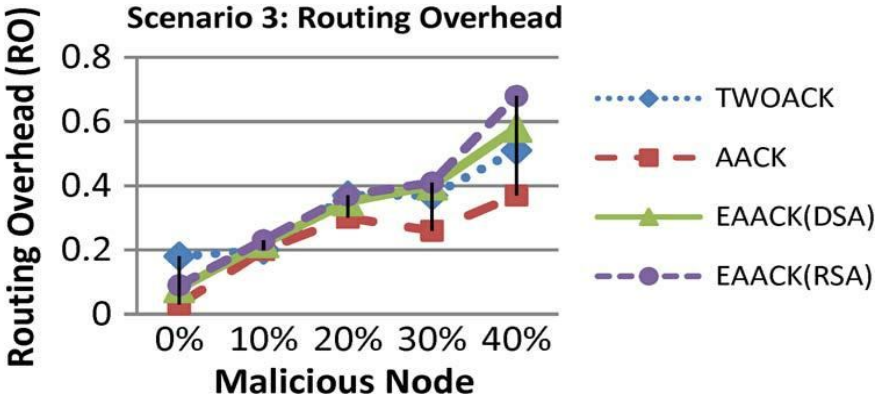

Fig 3- Routing overhead

Figure 2 shows, 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. 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. *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.

IV. 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 misbehaviour report .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 trade off 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.

V. FUTURE WORK

Secure data transmission is a critical issue for wireless networks. Clustering is an effective and practical way to enhance the system performance of Wireless Network. A secure data transmission for cluster based wireless networks, where the clusters are formed dynamically and periodically. Two Secure and Efficient data Transmission cluster-based CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for security, which is crucial for WSNs, while its security relies on the hardness of the discrete algorithm problem.

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?.
[2] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach,"
[3] L.Buttyan and J.Hubaux, "Stimulating cooperation in self organizing mobile ad hoc networks", ACM/Kluwer Mobile Network and Application (MONET) 8 (2003).
[4] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in *Communications in Computer and Information Science*,
[5] K.Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc net-works on the mobile value system".
[6] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbe-haviour in MANETs,".
[7] N.Kang, E.Shakshuki, and T. Sheltami, "Detecting forged acknowl-edgements in MANETs,"
[8] M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols".
[9] D.Barreto, Y.Liu, J.Pan and F.Wang."Reputation based participation enforcement for ad hoc network",http://www.standford.edu/~yl31/adhoc (2002).
[10] S.McCanne and S.Floyd, Network Simulator. Http://www.mash.cs.barkeley.edu/ns/.
[11] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc net-works on the mobile value system".
[12] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc net-works on the mobile value system".
[13] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in *Communications in Computer and Information Science.*