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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

An Efficient IDS for MANETs using EAACK

T.Murali[1], A.Nageswara Rao[2]

M.Tech Student, CSE, SV College of Engineering, Tirupati, India[1]

Professor. & Head, CSE, SV College of Engineering, Tirupati, India[2]

Abstract: A mobile ad hoc network (MANET) is a continuously self-administering, less-infrastructure network of mobile devices connected without wires. Each device in a MANET is free to move independently in more directions, and it can change its links to other devices frequently. The general challenge in building a MANET is equipping each device to continuously maintain the information required to its route traffic. Such networks may operate by itself or may be connected to the larger Internet. Every node works as both a transmitter and a receiver. They may contain one or multiple and different transceivers between nodes. This results in a highly – dynamic, autonomous topology .on individual layer like Application Layer (Malicious code, Repudiation) , Transport Layer(Session hijacking, Flooding) attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing this makes mantes vulnerable to a malicious attackers. we need to develop efficient intrusion-detection mechanisms to protect MANET from attacks. To overcome attacks on Mantes we have to provide more security by expanding MANETS into industrial applications based on improved technology and reduced hardware cost. Here we developed a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs has been developed. EAACK demonstrates higher malicious-behaviour-detection rates in certain circumstances while does not greatly affect the network performances.

Keywords: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (AACK) (EAACK), Mobile Ad hoc Network (MANET), Intrusion Detection System (IDS).

I. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such asPDAs, 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. Several standards for 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. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users.

One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. However, there is still 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.

***T.Murali**, M.Tech Student, Department of CSE, JNTUA,Anantapur/SV College of Engineering, Tirupati /India. (E-mail: muralitmr1227@gmail.com).*
***A.Nageswara Rao**, Professor & HOD, Department of CSE, JNTUA/Anantapur/SV College of Engineering, Tirupati /India. (E-mail:hod_cse_svce@svcolleges.edu.in).*

This problem has lead to a growing interest among the research community in *mobile ad hoc networks*, wireless networks comprised of mobile computing devices communicating without any fixed infrastructure**.** Due to their 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. 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. 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. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. RELATED WORK

The Watchdog/Pathrater is a solution to the problem of selfish (or "misbehaving") nodes in MANET. The system introduces two extensions to the DSR algorithm to mitigate the effects of routing misbehaviour: the Watchdog, to detect the misbehaving nodes and the Pathrater, to respond to the intrusion by isolating the selfish node from the network operation.

A. Intrusion Detection system 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, Intrusion Detection System (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 first time. IDSs usually act as the second layer in MANETs, and it is a great complement to existing proactive approaches and presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK.

B. watchdog:

Watchdog that aims to improve 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 intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviours in the network. Watchdog detects malicious misbehaviours by promiscuously listens to its next hop's transmission. If 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 researches and implementations have proved that the Watchdog scheme to be efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviours with the presence of

- ambiguous collisions,
- receiver collisions,
- limited transmission power,
- false misbehaviour report,
- collusion,
- Partial dropping.

C. TWOACK:

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 packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement 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).

The working process of TWOACK is demonstrated 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 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.

TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement 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.

D. AACK:
It is based on TWOACK Acknowledgement (AACK) similar to TWOACK,AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

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 misbehaviour report and forged acknowledgement packets. In fact, many of the existing IDSs in MANETs adopt acknowledgement based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is crucial to guarantee the acknowledgement packets are valid authentic. To address this concern to adopt digital signature in proposed scheme EAACK.

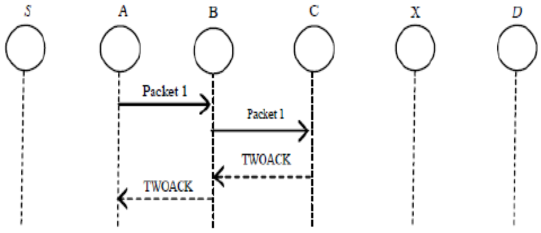

Figure1: Two ACK

III. PROBLEM DEFINITION

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. 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 misbehaviour attack. In this research work, our goal is to propose new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false 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

A. Scheme description:
In this section, we describe our proposed Enhanced Adaptive Acknowledgement (EAACK) scheme in details. The approach described in this research paper is based on our previous work, where the backbone of EAACK was proposed and evaluated through implementation. In this work, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: 1.Acknowledge (ACK), 2.Secure-Acknowledge (S-ACK) And 3. Misbehaviour Report Authentication (MRA). In order to distinguish different packet types in different schemes, we included a two-bit packet header in EAACK. Flowchart in fig 3 describing EAACK scheme. Please note that in my proposed scheme, I 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 acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver

B. AACK:
As discussed before, ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected. In Fig.3, in ACK mode, node S first sends out an ACK data packet *ad*1 *P* t o the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D Successfully receives *ad*1 *P*, node D is required to send back an ACK acknowledgement packet *ak*1 *P* along the same route but in a reverse order. Within a predefined time period, if node S receives *ak*1 *P* , 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.

C. S-ACK:
S-ACK scheme is an improved version of TWOACK scheme. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement 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. 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 to node F2. Then node F2 forwards this packet to node F3. When node F3 receives, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious.

Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S. 1 s adP1 s adP 1 s akP1 s akP. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehaviour report, EAACK requires the source node to switch to MRA mode and confirm this misbehaviour report. This is a vital step to detect false misbehaviour report in our proposed scheme. Detect misbehaving nodes in the network.

Node F1 first sends out S-ACK data packet *s ad*1 *P* to node F2. Then node F2 forwards this packet to node F3. When node F3 receives *s ad*1 *P* , as it is the third node in this three-node group, node F3 is required to send back an SACK acknowledgement packet*s ak*1 *P* to node F2. Node F2 forwards *s ak*1 *P* back to node F1. If node F1 does not receive this acknowledgement packet within predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehaviour report, EAACK requires the source node to switch to MRA mode and confirm this misbehaviour report. This is a vital step to detect false misbehaviour report in our proposed scheme.

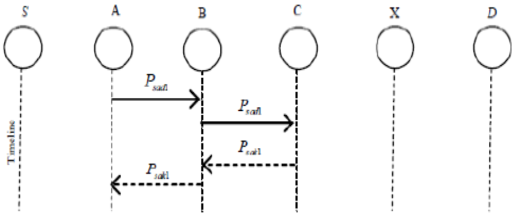

Figure2: s-ack scheme node C is required to send back an acknowledge packet t o node B

D. MRA:

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. False misbehaviour report can be generated by malicious attackers to falsely report that 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 MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other 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 misbehaviour reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

E. Digital Signature:

As discussed before, EAACK is an acknowledgement based IDS. All three parts of EAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviours in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement Packets, all of the three schemes will be vulnerable. With regarding to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgement 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 scheme in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANET.

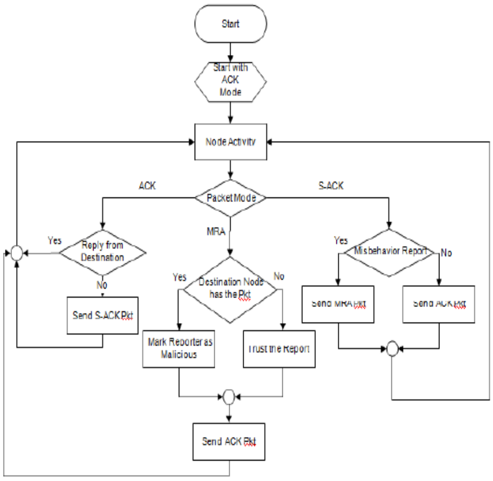

Figure 3: system flow of EAACK

F. Algorithm used:

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows: First, if $g = h^{(p-1)/q} \bmod p$ it follows that $g^q \equiv h^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem. Since $g > 1$ and q is prime, g must have order q. The signer computes.

$$s = k^{-1}(H(m) + xr) \bmod q$$

Thus

$$\begin{aligned} k &\equiv H(m)s^{-1} + xrs^{-1} \\ &\equiv H(m)w + xrw \pmod q \end{aligned}$$

Since g has order q (mod p) we have

$$\begin{aligned} g^k &\equiv g^{H(m)w} g^{xrw} \\ &\equiv g^{H(m)w} y^{rw} \\ &\equiv g^{u1} y^{u2} \pmod p \end{aligned}$$

Finally, the correctness of DSA follows from

$$\begin{aligned} r &= (g^k \bmod p) \bmod q \\ &= (g^{u1} y^{u2} \bmod p) \bmod q \\ &= v \end{aligned}$$

IV. CONCLUSION

In this paper we have presented novel IDS for MANET's named as EAACK. This has top priority in network security issues. Because it was specially designed to prevent from attackers to initiating forged acknowledge packets. We extend it by introducing digital signatures. 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 compared it against other popular mechanisms in different scenarios through simulations. The results generated positive performances.

REFERENCES

[1] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[2] 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.

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

[4] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[5] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling 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.

[6] 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.

[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 IEEEWorkshop 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," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile 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 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.

BIOGRAPHIES

T.Murali received B.Tech Degree from Annamacharya Institute of Technology & Sciences, Rajampet. He is currently pursuing M.Tech Degree in Computer Science Engineering specialization in SV College of Engineering, Tirupati, Andhra Pradesh, India.

A.Nageswara Rao received B.Tech Degree from CBIT, Osmaniya university, Hyderabad. M.Tech Degree in Computer Science at Central university, Hyderabad. He is currently working towards PhD in Data Mining specialization at Rayalaseema University, Kurnool, Andhra Pradesh, India, and working as professor & Head in the Dept. Of CSE, SV College of Engineering, Tirupati, Andhra Pradesh, India. He presented many research papers in National & International Conferences.