ISSN: 2321-7782 (Online)

Volume 3, Issue 5, May 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Enhancement to EAACK for improved MANET security

Pranjali. D. Nikam[1]
ME Computer Engineering
G.H.R.I.E.T., Savitribai Phule University, Pune
Pune – India

Vanita Raut[2]
ME Computer Engineering
G.H.R.I.E.T., Savitribai Phule University, Pune
Pune – India

Abstract: From past few decades there is a global trend in migrating form wired network to wireless network. Among all the wireless networks, Mobile Ad hoc Network (MANET) is one of the unique and most important applications. MANET is vulnerable to malicious attacks due to its open medium and wide distribution of nodes. To adjust to the growing trend of MANET in industrial applications, it is vital to address its potential security issues. A major threat to security in MANET is packet dropping attack. EAACK (Enhanced Adaptive Acknowledgement) scheme has been specially designed that demonstrates higher malicious –behaviour-detection rates under certain circumstances. In EAACK Digital signature has also been used to prevent the attackers from initiating forged acknowledgement attacks. Though EAACK overcomes the problems of false misbehaviour, limited transmission power and receiver collision, it increases network overhead due to use of digital signature. In this proposed system Elliptic Curve Cryptography (ECC) is used to further reduce the network overhead caused by digital signature.

Keywords: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET), Elliptic Curve Algorithm (ECC).

I. INTRODUCTION

Among all the wireless networks, Mobile Ad hoc Network (MANET) is one of the unique and most important applications. Irrespective traditional network architecture, MANET does not have a fixed network infrastructure. Every single node works both as a transmitter and a receiver. Nodes in same communication range directly communicate with each other. Nodes outside the communication range rely on their neighbours to relay messages.

MANET is vulnerable to malicious attacks due to its open medium and wide distribution of nodes. To adjust to the growing trend of MANET in industrial applications, it is vital to address its potential security issues. A new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs is proposed and implemented. Compared to contemporary approaches, EAACK demonstrates higher malicious- behaviour-detection rates in certain circumstances while does not greatly affect the network performances.

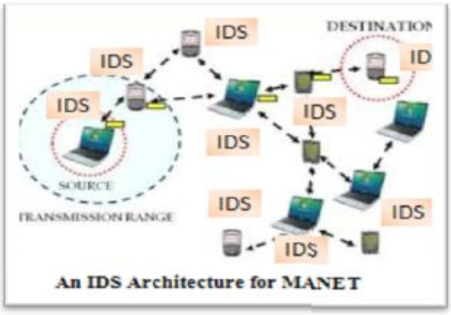

Fig.1 An IDS Architecture for MANET

II. LITERATURE SURVEY

A. IDS in MANETs

As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs presume that other nodes all the time work together with each other to transmit data. This hypothesis leaves the attackers with the opportunities to accomplish major impact on the network with just one or two compromised nodes.

To deal with this problem, an IDS should be added to improve the safety level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to entirely eradicate the probable damages caused by compromised nodes at the first time. IDSs generally operate as the second layer in MANETs, and they are a huge complement to existing proactive approaches [8]. Anantvalee and Wu [4] offered a very thorough study on modern IDSs in MANETs. In this segment, we primarily explain three existing approaches, that is, Watchdog [9], TWOACK [7], and Adaptive ACKnowledgment (AACK) [10].

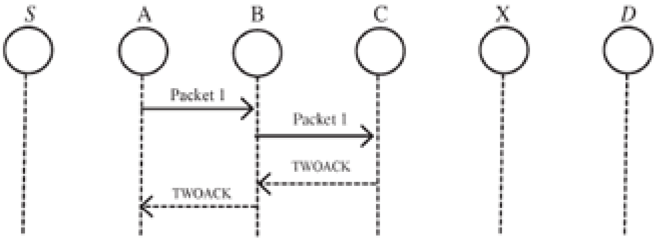

Fig. 2. Two ACK design: Each node is required to send back an acknowledgement packet to the node that is two hops away from it.

1. Watchdog:

Marti et al. [9] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network.

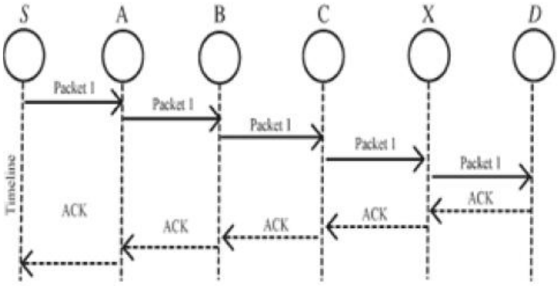

Fig. 3. ACK scheme: The destination node is required to send acknowledgement packets to the source node.

2. TWOACK:

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al. [13] 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. The TWOAC scheme is shown in Figure 2.

3. AACK:

Based on TWOACK, Sheltami et al. [10] proposed 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). The end-to-end acknowledgment scheme in ACK is shown in Figure 3.

4. EAACK:

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). EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehaviour, limited transmission power, and receiver collision. TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power.

B. ECC based Digital signature

Digital signature schemes can be used to provide the following basic cryptographic services:

1. Data veracity (the assurance that data has not been altered by unauthorized or unknown means)
2. Data origin authentication (the assurance that the source of data is as claimed)
3. Non-repudiation (the assurance that an entity cannot deny previous actions or commitments)

Elliptic Curve Digital Signature Algorithm is implemented over elliptic curve P-192 as mandated by ANSI X9.62 in C ++language. The Project contains necessary modules for domain parameters generation, key generation, signature generation, and signature verification over the elliptic curve.

ECDSA has three phases, key generation, signature generation, and signature verification.

III. System Implementation

Elliptic Curve Cryptography

1) Possibilities of adopting hybrid cryptography scheme to further decrease the network overhead caused by digital signature;

2) Look at the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys;

A. System Architecture

The Proposed approach 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 describe our proposed scheme in details. In this work, we extend it with the introduction of Elliptic Curve Based digital signature to prevent the attacker from forging acknowledgement packets. This scheme is consisted of three major parts, namely: ACKnowledge, Secure- ACKnowledge and Misbehavior Report Authentication (MRA). In order to differentiate different packet types in diverse schemes, we incorporated a two-bit packet header here. According to the Internet summary of DSR , there are six bits set aside in DSR header. We use two of the six bits to flag different A new intrusion detection system especially planned for MANETs, which resolves not only receiver conflict and restricted transmission power, but also the false misbehavior problem. This project is consisted of four major parts, namely: ACKnowledge, (ACK), Secure-ACKnowledge (S-ACK) and Misbehavior Report Authentication (MRA) and light weight based Elliptic curve digital signature and authentication to prevent the attacker from forging acknowledgement packets and authenticate each node as shown in Figure 4.

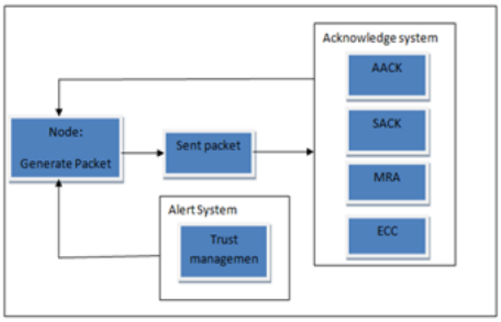

Figure: 4 Architecture illustration

B. Models

The modules are as follows,

1. Topology plan

   In this network, can have created the N nodes and N is provide by user as input. These nodes are used for communicating with each other indirectly to through the neighbor nodes.

2. Acknowledgement scheme

   ACK is basically an end-to-end acknowledgement scheme.

IV. System Model

To implement the desired simulation using ns3 network simulator the below given simulation parameters are required. Our simulation is conducted within the Network Simulator (NS) 3.20 environment on a platform with Fedora 19. The system is running on a min 20 GB of HDD, 3-GB RAM and I3 processor.

V. Results

Our algorithm result is analyzed by following parameters:

1. Throughput
2. Network overhead
3. End to End Delay
4. Energy Consumption

We can observe that our proposed scheme outperforms EEACK in all test scenarios related to End-to-End delay. We believe that this is because proposed work is the only scheme which is capable of reducing delay for every packet.

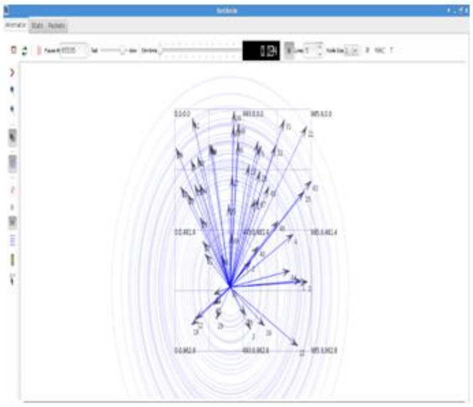

Figure: 5 Simulation of packet transfer through network

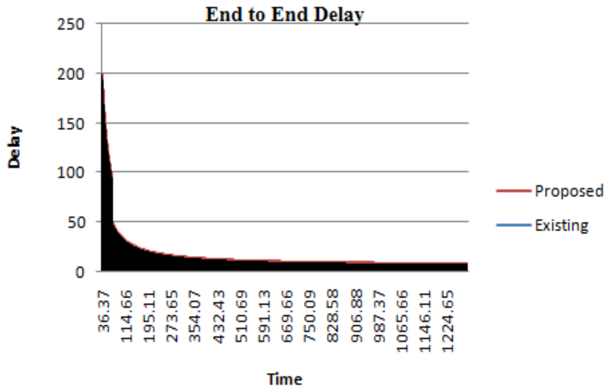

Figure: 6 Comparative result analysis

VI. Conclusion

To adjust to the growing trend of MANET in industrial applications, it is vital to address its potential security issues. A major threat to security in MANET is packet dropping attack. EAACK (Enhanced Adaptive Acknowledgement) scheme has been specially designed that demonstrates higher malicious –behavior -detection rates under certain circumstances. In EAACK Digital signature has also been used to prevent the attackers from initiating forged acknowledgement attacks. Though EAACK overcomes the problems of false misbehavior, limited transmission power and receiver collision, it increases network overhead due to use of digital signature. In this proposed system Elliptic Curve Cryptography (ECC) is used to further reduce the network overhead caused by digital signature.

Acknowledgement

I would like to thank Prof. Vanita Raut for her valuable guidance and support.

References

1. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE "EAACK—A Secure Intrusion-Detection System for MANETs"
2. Nitin Goyal1, Alka Gaba2 "A review over MANET- Issues and Challenges" Dept. of computer science and engineering, JMIT, Radaur, India
3. Pradeep Rai ,Shubha Singh "A Review of 'MANET's Security Aspects and Challenges" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010
4. Yogendra Kumar Jain, Rajesh Kumar Ahirwar "Secure Mobile Agent Based IDS for MANET" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4798-4805
5. B.Suruthi1 Mr.N.V.Rajeesh kumar.M.Tech2 An Enhanced Intrusion Detection System for MANETS using Hybrid Key Cryptography
6. MS. M.PONNRAJAKUMARI, ABIRAMI.S.P., 3KALYANI.R., 4SUBHASHRI.M., 5SUCHITHRA.R A SECURE INTRUSION DETECTION USING IMPROVED EAACK IN MANETS
7. J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.
8. B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
9. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.
10. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
11. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.
12. 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.
13. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
14. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.
15. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs,"

AUTHOR(S) PROFILE

Ms. Pranjali D Nikam, received M.E degree in Computer Engineering from GHRIET, Pune. Since 2010 she is working as lecturer in GHRIET, Pune in Computer department.