Asian Journal of Applied Science and Technology (AJAST)
(Open Access International Journal) Volume 1, Issue 4, Pages 58-60, 2017

ENHANCED ADAPTIVE ACKNOWLEDGEMENT BASED IDS-A REVIEW

K.Sujatha[1], Dr.R.Reka[2], S.Venkata Lakshmi[3] and K.Sathyamoorthy[4]

[1]*Professor, Department of CSE, Panimalar Institute of Technology, Chennai, Tamilnadu, India.*
[2]*Professor, Department of IT, Panimalar Institute of Technology, Chennai, Tamilnadu, India.*
[3]*Associate Professor, Department of CSE, Panimalar Institute of Technology, Chennai, Tamilnadu, India.*
[4]*Associate Professor, Department of CSE, Panimalar Institute of Technology, Chennai, Tamilnadu, India.*

Article Received: 12 May 2017 *Article Accepted: 24 May 2017* *Article Published: 28 May 2017*

ABSTRACT

Security has become a question in Mobile Ad-hoc networks due to their dynamic topology, mobility, scalability and shared resources. Intrusion detection techniques are introduced to mitigate the attacks of compromised nodes and acts as a second wall of defense. EAACK is a secure intrusion detection technique that is specially designed to enhance the security level in MANET's, compared to contemporary intrusion detection techniques. MANET is a self-configuring network formed automatically by a collection of mobile nodes. No fixed infrastructure or centralized management. Characteristics of MANET are Autonomous and infrastructure less, Multi-hop routing, Dynamic network topology, Device heterogeneity, Energy constrained operation, Bandwidth constrained variable capacity links, Limited physical security, Network scalability, Self-creation and self-organization and self-administration.

Keywords: Oxidation, Cinnamic acid, Quinolinium fluorochromate and Kinetics.

1. INTRODUCTION

Due to their natural mobility and scalability, wireless networks are always preferable 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. A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or indirectly depending on other nodes. In recent years, the use of mobile ad hoc network (MANET) has been widespread in many applications, including some critical mission applications and as such security has become one of the major concerns in MANET. MANET does not require a fixed infrastructure and MANET originally developed on military use. However the open medium and wide distributions of nodes make to various types of malicious attacks. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use recovery.

However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop an efficient intrusion detection mechanism to product MANET from attacks. In this paper, we propose and implement a new intrusion detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANET and Compared to all contemporary approaches. The results will be positive performances of WATCHDOG, TWOACK and AACK in the cases are receiver collision, limited transmission power and false misbehaviour report.

2. IDS APPROACHES

In this section, we mainly describe four existing approaches for IDS namely, Watchdog, TWOACK, Adaptive Acknowledgment (AACK), and EAACK.

2.1 Watchdog

It is very popular and highly efficient IDS for improving the throughput of network with the presence of malicious nodes. These IDS can be classified into two methods such as Watchdog and Path rater. It is responsible for discovering malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by listening to its next hop's transmission in the network. If a Watchdog IDS 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 value, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. The Watchdog-IDS fails to discover malicious nodes in the following situations: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

2.2 TWOACK

It is another important IDS TWO-ACK for discovering malicious nodes in MANETs. The main aim of this ID to resolve the receiver collision and limited transmission power problems of Watchdog, TWO-ACK detects misbehaving links by acknowledging every data packet transmitted over every 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 acknowledgment packet to the node that is two hops away from it down the route. TWO-ACK is required to work on routing protocols such as Dynamic Source Routing. The TWOACK IDS effectively processes the receiver collision and limited transmission power problems indicated by Watchdog. However, the acknowledgment 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.

2.3 AACK

It is same as TWO-ACK IDS, AACK IDS is an acknowledgment-based network layer IDS. It can be treated as a combination of an ID called TACK (identical to TWO-ACK) and an end-to-end acknowledgment IDS called Acknowledge (ACK). Compared to TWO-ACK IDS, AACK IDS reduced network overhead. The source node sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node along the reverse order of the same path. Within a predefined time slot, if the source node receives this ACK packet, then the packet transmission from node Source to node Destination is successful. 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 fake ACK packets. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWO-ACK and AACK. The functions of such detection schemes all largely depend on the ACK packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

2.4 EAACK

Enhanced Adaptive Acknowledgment IDS (EAACK) is based on both DSA and RSA algorithm. The three main parts of the EAACK scheme are ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). EAACK is an acknowledgement based IDS. This scheme uses the digital signature method to prevent the attacker from forging acknowledgment packets. Before the acknowledgement packets sent out EAACK requires the whole acknowledgement packets are digitally signed and verified by its receiver until they are accepted.

3. CONCLUSIONS

The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misconduct report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our new research to incorporate digital signature in our proposed working scheme.

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 technology, 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,in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659.666.

[3] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Computer Sci., vol. 3, no. 8, pp. 574–582, 2007.

[4] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[5] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

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