Middle-East Journal of Scientific Research 19 (9): 1205-1208, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.19.9.11218

EAACK: Enhanced Adaptive Acknowledgment for MANET

G. Micheal and A.R. Arunachalam

Department of Computer Science and Engineering,
Bharath University, Chennai, India

Abstract: 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. 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, limitedtransmission power and false misbehavior eport.

Key words: MANET · Enhanced Adaptive Acknowledgment · Digital Signature · AACK

INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network that isformed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. A MANET with the characteristics described above was originally developed for military purposes, as nodes are scattered across a battlefield and there is no infrastructure to help them form a network. An IDScollects activity information and then analyzes it to determine whether the reare any activities that violate the security rules [1]. we haveproposed a novel IDS named EAACK protocol specially designedfor MANETs and compared it against other popular mechanisms in different scenarios through simulations. Theresults demonstrated positive performances against Watchdog,TWOACK and AACK in the cases of receiver collision, limited transmission power and false misbehavior report.

Watchdog: Watchdog that aims to improve the throughput of network withthe presence of malicious nodes. In fact, the Watchdog schemeis consisted of two parts, namely, Watchdog and Pathrater [2]. Watchdog serves as IDS for MANETs. It is responsiblefor detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog nodeoverhears that its next node fails to forward the packet withina certain period of time, it increases its failure counter. Whenevera 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 [3].

TWOACK: With respect to the six weaknesses of theWatchdog scheme, many researchers proposed new approachesto solve these issues. TWOACK proposed one of the most important approaches among them. Onthe contrary to many other schemes, TWOACK is neither anenhancement nor aWatchdog-based scheme. Aiming to resolvethe receiver collision and limited transmission power problemsof Watchdog, TWOACK detects misbehaving links byacknowledging every data packet transmitted over every threeconsecutive nodes along the path from the source to the destination [4-6]. The TWOACK scheme successfully solves the receiverCollision and limited transmission power problems posed byWatchdog. However, the acknowledgment process required inevery packet transmission process added a significant amount ofunwanted network

Corresponding Author: G. Micheal, Department of Computer Science and Engineering,
Bharath University, Chennai, India.

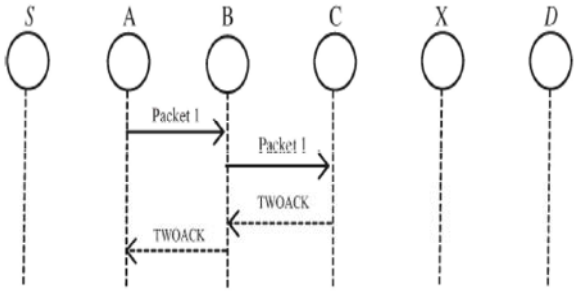

Fig. 1: TWOACK scheme: Each node is required to send back an acknowledgmentpacket to the node that is two hops away from it.

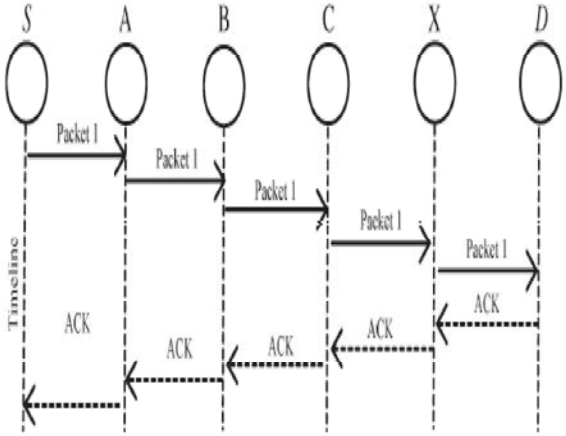

Fig. 2: ACK scheme: The destination node is required to send acknowledgmentpackets to the source node.

overhead. Due to the limited battery powernature of MANETs, such redundant transmission process caneasily degrade the life span of the entire network.

AACK: a new scheme called AACK. Similar to TWOACK,AACK is an acknowledgment-based network layer schemewhich can be considered as a combination of a scheme calledTACK (identical to TWOACK) and an end-to-end acknowledgmentscheme called Acknowledge (ACK).

Compared toTWOACK, AACK significantly reduced network overheadwhile still capable of maintaining or even surpassing the samenetwork throughput.Compared toTWOACK, AACK significantly reduced network overheadwhile still capable of maintaining or even surpassing the samenetwork throughput [7-8].

Literature Survey: A Survey on Intrusion Detection Systems in MANET [2]: Intrusion means any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource.

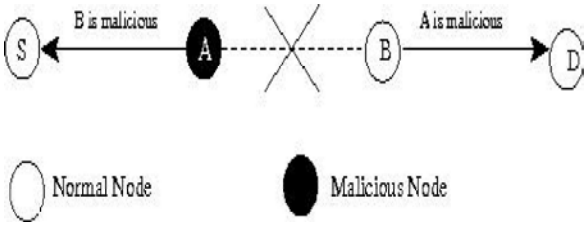

Fig. 3: Malicious node

Intrusion Prevention is the primary defense because the primary step is to make the systems safe from attacks by using passwords, biometrics etc. Even if intrusion prevention methods are used, the system may be subjected to some vulnerability. So we need a second wall of defense known as Intrusion Detection Systems (IDSs), to detect and produce responses if necessary [9-14].

Enhanced IDS for Discovering Malicious Nodes in MANET [1]: Many intrusion detection systems have been proposed and most of them are tightly related to routing protocols, such as Watchdog/Pathrater and Route-guard. These solutions include two parts: intrusion detection (Watchdog) and response (Pathrater and Route-guard). Watchdog resides in each node and is based on overhearing.

Through overhearing, each node can detect the malicious action of its neighbours and report other nodes. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance. They had we overcome the weakness of Watchdog and introduce our intrusion detection system called ExWatchdog. 2.3 Secure Trust Metadata Management for MANET [3]: A trust management framework [2] is useful to ensure proper functioning of a mobile ad-hoc network (MANET). Trust metadata created by individual nodes, based on their observation of the behavior of other nodes in their vicinity, is required to be accessible to a trust authority (e.g., the network administrator) for prompt decision making (e.g., revoking malicious nodes). In this work, for security and scalability reasons, we propose a secure semantics-aware trust metadata management scheme to partition and store an information network of trust metadata of nodes in a MANET. That is, trust metadata is securely propagated to and stored at certain geographic locations inside the network itself, based on its semantics. 2.4SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks[3]:This paper design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-

Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability and to guard against Denial of-Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use e?cient one-way hash functions and do not use asymmetric cryptographic operations in the protocol [15]. SEAD performs well over the range of scenarios we tested and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.2.5 Dynamic Source Routing in Ad Hoc Wireless Networks [4]: This paper presents a protocol for routing in ad hoc networks that uses dynamic source routing. The protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates [16].

Existing System: The network performance was identified by the received signal strength at the destination. The path from source to destination was vulnerable to spoofing attacks. There was no method proposed here to detect the presence of attackers. So overall throughput of the network was minimum and the network performance was degraded [17].

Proposed System: The EEACK consist of three majorparts as ACK, SACK and MRA.

- ACK: ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme inEAACK, aiming to reduce network overhead when no networkmisbehavior is detected.
- SACK: The S-ACK scheme is an improved version of the TWOACKScheme. The principle is to let everythree consecutive nodes work in a group to detect misbehavingnodes. For every three consecutive nodes in the route, the thirdnode is required to send an S-ACK acknowledgment packet tothe first node. The intention of introducing S-ACK mode is todetect misbehaving nodes in the presence of receiver collisionor limited transmission power [18-20].
- MRA: To initiate the MRA mode, the source node first searches itslocal knowledge base and seeks for an alternative route to thedestination node.

Fig. 4: EAACK Scheme

If there is no other that exists, the source nodestarts a DSR routing request to find another route. Due to thenature of MANETs, it is common to find out multiple routestwo nodes.

By adopting an alternative route to the destination node, wecircumvent the misbehavior reporter node. When the destinationnode receives an MRA packet, it searches its local knowledgebase and compares if the reported packet was received. If itis already received, then it is safe to conclude that this is a falsemisbehavior report and whoever generated this report is markedas malicious. Otherwise, the misbehavior report is trusted andaccepted.EAACK is capable ofdetecting malicious nodes despite the existence of false misbehaviorreport.

CONCLUSION

Packet-dropping attack has always been a major threat tothe security in MANETs. We haveproposed a novel IDS named EAACK protocol specially designedfor MANETs and compared it against other popularmechanisms in different scenarios through simulations. Theresults demonstrated positive performances against Watchdog, TWOACK and AACK in the cases of receiver collision, limitedtransmission power and false misbehavior report.

REFERENCES

1. Singh, A., M. Maheshwari and N. Kumar, 2011. Security And Trust Management In Manet, Incommunications In Computer And Information Science, Vol. New York: Springer-Verlag, 147(3): 384-387.
2. Anantvalee, T. and J. Wu, 2008. A Survey On Intrusion Detection In Mobile Ad Hoc Networks, In Wireless/Mobile Security. New York: Springer-Verlag.
3. Hu, Y., D. Johnson and A. Perrig, 2002. Sead: Secure Efficient Distance Vector Routing For Mobile Wireless Ad Hoc Networks, In Proc. 4th Ieee Workshopmobile Comput. Syst. Appl., pp: 3-13.
4. Johnson, D. and D. Maltz, 1996. Dynamic Source Routing In Ad Hoc Wireless Networks, In Mobile Computing. Norwell, Ma: Kluwer, 5: 153-181.
5. Nasser, N. and Y. Chen, Jun, 24-28, 2007. Enhanced Intrusion Detection Systems For Discovering Malicious Nodes In Mobile Ad Hoc Network, In Proc. Ieee Int. Conf. Commun., Glasgow, Scotland, pp: 1154-1159.
6. Akbani, R., T. Korkmaz and G.V.S. Raju, 2012. Mobile Ad Hoc Networksecurity, In Lecture Notes In Electrical Engineering. New York: Springer-Verlag, 127: 659-666.
7. Jayakumar, G. and G. Gopinath, 2007. Ad Hocmobile Wireless Networks Routingprotocol-A Review, J. Comput. Sci., 3(8): 574-582.
8. Sun, B., 2004. Intrusion Detection In Mobile Ad Hoc Networks, Ph.D. Dissertation, Texas A and M Univ., College Station, Tx.
9. Stanoevska-Slabeva, K. and M. Heitmann, Jun. 2003. Impact Of Mobile Ad-Hoc Networkson The Mobile Value System, Inproc. 2nd Conf. M-Bus., Vienna, Austria.
10. Hu, Y., A. Perrig and D. Johnson, 2002. Ariadne: A Secure On-Demand Routingprotocol For Ad Hoc Networks, In Proc. 8th Acm Int. Conf. Mobicom,Atlanta, Ga, pp: 12-23.
11. Kumaravel, A., 2013. An Application Of Non-Uniform Cellular Automata For Efficient Cryptography, Xplore, (S): 1200-1205.
12. Kumaravel, A., 2013. Routing Algorithm Over Semi-Regular Tessellations, Xplore, pp: (S): 1180-1184.
13. Kumaravel, A., 2013. Algorithm For Automaton Specification For Exploring Dynamic Labyrinths, Indian Journal Of Science And Technology, 6: 5.
14. Kumaravel, A., May 2013. Application Of Non-Uniform Cellular Efficient Cryptography Automata, Indian Journal Of Science And Technology, 6(5s): 4561-4566.
15. Kumaravel, A., May 2013. Introducing An Efficient Programming Paradigm For Object-Oriented Distributed Systems, Indian Journal Of Science And Technology, 6(5s): 4597-4603.
16. Tatyana Aleksandrovna Skalozubova and Valentina Olegovna Reshetova, 2013. Leaves of Common Nettle (Urtica dioica L.) As a Source of Ascorbic Acid (Vitamin C), World Applied Sciences Journal, 28(2): 250-253.
17. Rassoulinejad-Mousavi, S.M., M. Jamil and M. Layeghi, 2013. Experimental Study of a Combined Three Bucket H-Rotor with Savonius Wind Turbine, World Applied Sciences Journal, 28(2): 205-211.
18. Vladimir G. Andronov, 2013. Approximation of Physical Models of Space Scanner Systems World Applied Sciences Journal, 28(4): 528-531.
19. Naseer Ahmed, 2013. Ultrasonically Assisted Turning: Effects on Surface Roughness World Applied Sciences Journal, 27(2): 201-206.
20. Tatyana Nikolayevna Vitsenets, 2014. Concept and Forming Factors of Migration Processes Middle-East Journal of Scientific Research, 19(5): 620-624.