Volume : 3 | Issue : 1 | January 2014 • ISSN No 2277 - 8179

Securing Manet to Avoid Intrusion Using Enhanced Adaptive Acknowledgment Technique

Engineering

KEYWORDS : Mobile Ad hoc NETwork, Digital signature, digital signature algorithm, routing misbehavior, security

Mr. R. Vijayakumar	Department of Computer Science and Engineering, Muthayammal Engineering College, Namakkal, Tamilnadu, India
Mr. R. Muralidharan	Department of Computer Science and Engineering, Muthayammal Engineering College, Namakkal, Tamilnadu, India
Mr. P. Dhanarasan	Department of Computer Science and Engineering, Muthayammal Engineering College, Namakkal, Tamilnadu, India

ABSTRACT

Security has become an important part in Mobile Adhoc Networks because of their dynamic mobility, scalability and shared resources. MANETs is a collection of mobile nodes and it does not require a fixed infrastructure. So it acts as a dynamic topology for many applications. MANETs are highly vulnerable for attacks because of their open medium, rapidly changing topology, lack of centralized monitoring. Both Watchdog and TWOACK methods are not sufficient for protect MANETs in the cases of receiver collision, limited transmission power and false misbehavior report. To overcome such attacks the proposed technique is a secure intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs

1. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users. 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. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in mobile ad hoc networks (MANETs), wireless networks comprised of mobile computing devices communicating without any fixed infrastructure.

2. NETWORK MODEL

INTRUSION DETECTION SYSTEM (IDS) ARCHITECTURE

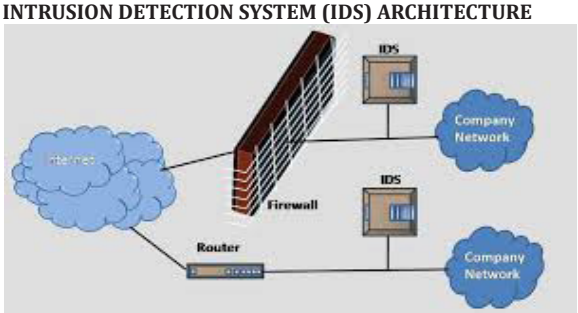

Fig.2.1. Intrusion Detection System (IDS)

MANET has features such as an open medium, dynamic changing topology, and the lack of a centralized monitoring and management point, many of the intrusion detection techniques developed for a fixed wired network are not applicable in MANET. Zhang [1] gives a specific design of intrusion detection and response mechanisms for MANET. Marti [2] proposes two mechanisms: watchdog and path rater, which improve throughput in MANET in the presence of nodes that agree to forward packets but fail to do so.

3. RELATED WORK

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 the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [3]. In this section, we mainly describe two existing approaches, namely,

1. Watchdog [4],
2. TWOACK [5].

3.1 WATCHDOG

In [5], Marti et al. proposed a reputation-based scheme. Two modules called watchdog and pathrater are implemented at each node, to detect and mitigate, respectively, routing misbehaviors in MANETs. Nodes operate in a promiscuous mode wherein, the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet or not. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination. Therefore, each intermediate node in the path should know who the next hop node is. Below fig.3.1 shows how the watchdog works.

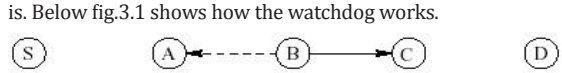

Fig.3.1. How watchdog works

MANET IDSs are either based on or developed as an improvement to the Watchdog scheme [6]. Watchdog scheme fails to detect malicious misbehaviors with the presence of the following:

1. Ambiguous Collisions:

A packet collision occurs at the monitoring node.

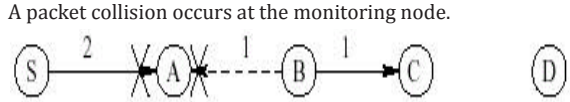

Fig.3.2. Ambiguous collision

2. Receiver Collisions:

A packet collision occurs at the receiver. Both nodes B and D are trying to send packet 1 and packet 2, respectively, to node C at the same time.

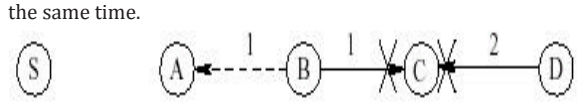

Fig.3.3. Receiver collision

3. Limited Transmission Power:

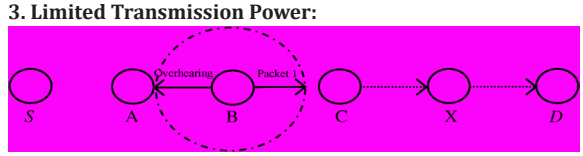

Fig.3.4. Limited transmission power

Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

4. False Misbehavior Report:
The Node A sends back a misbehavior report even though node B forwarded the packet to node C.

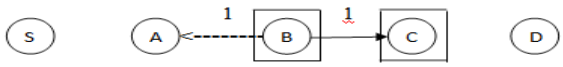

Fig.3.5. Collusion

6. Partial Dropping:
Node keeps its tally just below the threshold and never is labeled as misbehaving.

3.2 TWOACK
The TWOACK scheme can be implemented on top of any source routing protocol such as DSR. This follows from the fact that a TWOACK packet derives its route from the source route established for the corresponding data packet. The TWOACK scheme uses a special type of acknowledgment packets called TWOACK packets, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets.

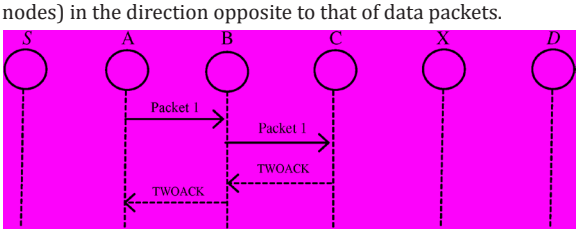

Fig.3.6. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

4. PROPOSED SYSTEM
My proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely receiver collision, limited transmission power and false misbehavior. In this section, we discuss these three weaknesses in details.

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 [7], where the backbone of EAACK was proposed and evaluated through implementation.

EAACK is consisted of three major parts, namely:
1. Acknowledgment (ACK),
2. Secure-Acknowledgment (S-ACK) and
3. Misbehavior Report Authentication (MRA).

In order to distinguish different packet types in different schemes, we included a two-bit packet header in EAACK.

Acknowledgment:
ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, 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.

Secure-Acknowledgment:
S-ACK scheme is an improved version of TWOACK scheme proposed by Liu et al. [8]. 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. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

Misbehavior Report Authentication:
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 misbehavior report. 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 misbehavior reporter node.

5. CONCLUSION AND FUTURE WORK
Malicious 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 designed 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 misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. The future work is to evade or minimize partial dropping in communication of mobile nodes.

REFERENCE

[1] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003. | [2] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,"Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p.57.1, January 2003. | [3] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004. | [4] 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. | [5] 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. | [6] 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., 2004, pp. 747–752. | [7] N. Kang, E. Shakshuki andT. Sheltami. Detecting Misbehaving Nodes in MANETs. The 12th International Conference on Information Integration and Web-based Applications & Services (WAS2010), ACM, pp. 216-222, November, 8-10, Paris, France, 2010. | [8] Jin-Shyan Lee, "A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 4, pp. 1835-1841, April 2008. |