Volume 4, No. 4, April 2013

Journal of Global Research in Computer Science

ISSN-2229-371X

REVIEW ARTICLE

Available Online at www.jgrcs.info

A SURVEY OF INTRUSION DETECTION FOR AD-HOC NETWORK

*1Jacob Abraham, 2V.Arun Prasath,3G.Michael
*1The Computer Science Department, Bharath University, Chennai, TamilNadu, India
jacobabraham01@gmail.com1
2 The Computer Science Department, Bharath University, Chennai, TamilNadu, India
vel.arunprasath@gmail.com3
The Computer Science Department, Bharath University, Chennai, TamilNadu, India
micmgeo@yahoo.co.in3

Abstract- Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. MANET does not require a fixed network formation, since every single node works as both a sending and a receiving messeges and it communicate with each other. Nodes communicate directly with each other when they are both within the same communication range. we implement a new intrusion detection system named Enhanced Adaptive ACKnowledgement (EAACK) designed for MANETs.

INTRODUCTION

Due to its natural mobility and scalability, wireless networks are always preferred since the first day of its invention. Thanks to the improved technology and reduced costs, wireless networks have1 gained much more preferences over wired networks in the past few decades By definition, MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. Industrial remote access and control via wireless network 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 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 its radio range. In contrary to the traditional wireless network, MANET has a decentralized network 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 mission critical 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-created disasters, military differences and medical emergency.

Thanks to these unique characteristics, Mobile Ad-hoc network is becoming commmonly used in the industry. Anyway, seeing the fact that MANET is popular among mission critical 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. Especially 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, traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop intrusion detection system specially designed for MANETs. Many research efforts have been devoted to such research topic . In the next section, we mainly concentrate on discussing the background information required for understanding this research topic.

Existing System:

As discussed before, due to the limitations of most MANET routing protocols nodes in Mobile Ad-hoc network's finds 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 get into 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. Jie et al. presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK.

a. ***Watchdog:*** Marti et al. proposed a scheme named 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 misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. If 'Watchdog' node is intimated that it is 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 pre-defined 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 . Nevertheless, as pointed out by Marti *et al*, Watchdog scheme fails to detect malicious misbehaviors with the presence of 1. receiver collisions, 2. Ambiuous collisions, 3. limited transmission power, 4. false misbehavior report, 5. collusion, and 6. partial dropping. We discuss these weaknesses with further detail in Section III.

b. ***TWOACK:*** With respect to the six weaknesses of Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al. is one of the most important one among them. On the contrary to many other schemes, 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. The same process applies to each three consecutive nodes along rest of the route. 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. However, many researches are working in energy harvesting to deal with this problem.

c. ***AACK:*** Based on TWOACK, Sheltami et al. proposed a new scheme called Adaptive ACKnowledgement (AACK). Similar to TWOACK, AACK is an acknowledgement-based network layer scheme which can be considered as a combination of a scheme called TACK (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. The end-to-end acknowledgement scheme in ACK is demonstrated. In ACK scheme, the source node S sends out Packet 1 without any overhead except two bit of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgement packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgement packet, then the packet transmission from node S to node D is successful. Otherwise the 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 misbehavior 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 and authentic. To address this concern, we adopt digital signature in our proposed scheme EAACK.

Proposed System:

The Proposed approach EAACK 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 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: ACKnowledge (ACK), Secure-ACKnowledge (S-ACK) and Misbehavior Report Authentication (MRA). In order to distinguish different packet types in different schemes, we included a two-bit packet header in EAACK. According to the Internet draft of DSR , there are six bits reserved in DSR header. In EAACK, we use two of the six bits to flag different A new intrusion detection system specially designed for MANETs, which solves not only receiver collision and limited transmission power, but also the false misbehavior problem. EAACK is consisted of three major parts, namely: ACKnowledge

(ACK), Secure-ACKnowledge (S-ACK) and Misbehavior Report Authentication (MRA). And we extend it with the digital signature to prevent the attacker from forging acknowledgement packets.

Architecture Diagram:

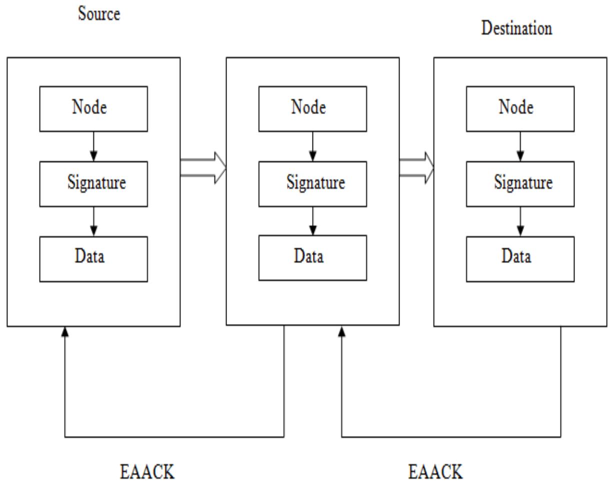


Figure: 1

Modules:

The modules are as follows,

a. Network Topology
b. Ack and S-Ack Scheme
c. MRA and Digital Signature Scheme

Network Topology:

In our first module, we have to establish the Network. In this network, can have created the N nodes. These nodes are used to communicating each other indirectly to through the neighbor nodes. Using multicast socket, all nodes are used to detect the neighbor nodes.

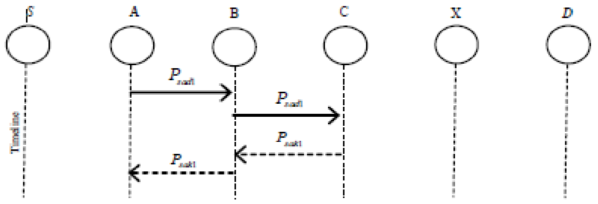
Ack and S-Ack Scheme:

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 misbehavior is detected. 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.

MRA and Digital Signature Scheme:

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. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious.



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. The Digital Signature requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted. The goal is to find the most optimal solution for using digital signature in MANETs.

FUTURE ENHANCEMENT

To increase the merits of our research work, we plan to investigate the following issues in our future research:

a. Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.
b. Examine the possibilities of adopting key exchange mechanism to eliminate the requirement of pre-distributed keys.
c. Testing the performance of EAACK in real network environment instead of software simulation.

CONCLUSION

Packet dropping attack has always been a major threat to the security in MANETs. In this research work, we proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulation. The results demonstrated positive performances against Watchdog, TWOACK and AACK in the cases of receiver collision and limited transmission power and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating a forged acknowledgement attacks, we extended our research to incorporate digital signature in our proposed scheme. Although it generates more routing overhead in some cases, as demonstrated in our experiment, it can vastly improve the network's packet delivery ratio when the attackers are smart enough to forge acknowledgement packets. We think this trade-off is worthwhile when network security is of top priority. In order to seek the optimal digital signature algorithms in MANETs, we implemented both DSA and RSA scheme in our simulation. Eventually, we arrived to the conclusion that DSA scheme is more suitable to be implemented in MANETs.

REFERENCE

[1]. P. Minet, T. Dang K. Al Agha, M.-H. Bertin, , A. Guitton, , T. Val, J.-B. Viollet, "Which Wireless Technology for Industrial Wireless Sensor Networks? The Development of OCARI Technol," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 4266-4278, Oct 2009.

[2]. R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Network Security", Lecture Notes in Electrical Engineering, vol. 127, pp. 659-666, Springer, 2012 – here1

[3]. R.H. Akbani, S. Patel, D.C. Jinwala. “DoS Attacks in Mobile Ad Hoc Networks: A Survey”, the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012. – here1

[4]. T. Anantvalee and J. Wu. A Survey on Intrusion Detection in Mobile Ad hoc Networks. In Wireless/Mobile Security, Springer, 2008.

[5]. L. Buttyan and J.P. Hubaux. Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.

[6]. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, L. Benini, "Modeling and Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 7, pp. 2759-2766, July 2008.

[7]. V. C. Gungor, G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approac," IEEE Trans. on Industrial Electronics, 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 the Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-13, 2002.

[9]. Y. Hu, A. Perrig, and D. Johnson. ARIADNE: A Secure On-Demand Routing Protocol for Ad hoc Networks. In the Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom’02), pp. 12-23, Atlanta, GA, 2002.

[10]. G. Jayakumar and G. Gopinath. Ad Hoc Mobile Wireless Networks Routing Protocol – A Review. In Journal of Computer Science 3(8): 574-582, 2007.

[11]. D. Johnson and D. Maltz. Dynamic Source Routing in Ad hoc Wireless Networks. Mobile Computing, Kluwer Academic Publishers, Chapter 5, pp. 153-181, 1996.

[12]. N. Kang, E. Shakshuki andT. Sheltami. Detecting Misbehaving Nodes in MANETs. The 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), ACM, pp. 216-222, November, 8-10, Paris, France, 2010.

[13]. N. Kang, E. Shakshuki andT. Sheltami. Detecting Forged Acknowledgements in MANETs. The 25th International Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society, Biopolis, Singapore, March 22-25, 2011.

[14]. K. Kuladinith, A.s Timm-Giel and C. Görg. Mobile Ad-Hoc Communications in AEC industry. In Journal of Information Technology in Construction Vol. 9, pp. 313-323, 2004.

[15]. 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.