Effective Intrusion Detection Scheme in Mobile Ad-Hoc Networks

Sonal Soni
M.E. Student SDBCT Indore

Arjun Parihar
Asst, Prof., SDBCT Indore

ABSTRACT
Mobile ad-hoc network needs to take major concern of security due to vulnerable open environment and non-stationary mode. Mostly, offenders focus to attack on victim using these venerable points to affect resources and performance of the networks. Kinds of attack targeted on victim nodes which are influence resources actively and passively. Several works have been done to detect and mitigate such kind of attacks, but still some more work required. In this paper, different activity of intrusion and IDS Schemes are discussed.

Keywords
Mobile Ad-hoc Networks, IDS, Watchdog, Pathrater, AACK

1. INTRODUCTION
In ad-hoc network each node has facility to move anywhere in network area without co-ordination, thus mobility of nodes make network vulnerable in security aspect. Security is one of the most important constraints f1or the ad hoc network performance. This vulnerability invite attacker to attacking several kinds of attacks on the network resources. These attacks impact on network throughput, performance and lifetime. A lot of research have been done against attacks and required more research to defend the network resources from different attacks by detecting and preventing data from detected attack. Efforts are putting to improve the network security mechanism for smooth network operations against intrusion. Infrastructure-less property of mobile ad-hoc network attracts it in various areas. Some of them discussed here.

1.1 Collaborative Work
For some business environments, the need for collaborative computing might be more important outside office environments than inside [1]. After all, it is often the case where people do need to h1ave outside meetings to cooperate and exchange information on a given project.

1.2 Crisis-management Applications
These occure, for example, as a result of natural disasters where the whole communications infrastructure is in disorder. Restoring communications quickly is essential. By using ad hoc networks, a communication channel could be set up in hours in spite of days/weeks required for wire-line communications.

1.3 Personal Area Networking and Bluetooth
A personal area network (PAN) is a short- range, localized network where nodes are generally associated with a given person [2]. These nodes could be attached to someone's pulse watch, belt, and so on. In these scenarios, mobility is only a major consideration when interaction among several PANs is necessary.

2. RELATED WORK
During the last few years various authors have published so many documents to forward the attacks detection work. According to most of them the work can be done effectively by taking multiple environmental factors to get the accurate analysis & design of methodologies. Some of them is given as follows:

Marti et al. [3] introduced Watchdog technique as well as Pathrater techniques in 2000 that increase network performance within existence of malicious nodes. Watchdog uses to find malicious nodes in a network that agree to forward packets but fail to do so, while Pathrater technique uses to bypass these malicious nodes in a route path in the future transmission. The integrating of Watchdog and Pathrater techniques improve network performance significantly [3] in MANETs. Watchdog technique detects the malicious nodes by exercising promiscuous mode, where each node listens to its near by nodes transmissions. If the next node in a route path fails to pass ahead the sent packet, It increases its failure counter. Then it determines the node as malicious if the failure counter go beyond a certain predefine threshold. As a result, the Pathrater technique bypasss this node in the future transmission by cooperating with routing protocol to choose distant path from source to destination based on the used algorithm. Even though Watchdog and Pathrater techniques are able to detect malicious nodes at forward level contrary to the link level, it may fail to detect malicious nodes within the existence of: 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior report, 5) collusion (collaborative) of malicious nodes, and 6) partial dropping.

The TWOACK [4] technique is a network layer acknowledgment scheme introduced by Balakrishnan et al. TWACK replace Watchdog scheme by dealing with two of its deficiencies, named, receiver collision and limited transmission power. In TWOACK, when node send a packet to its nearby node in a route path, it has to validate whether the packet successfully received by the node that is two hops from it. This achieved by approving every data packet sent from source to destination over every three continuous nodes along the path. As shown in figure 1, node B receives packet 1 from A and forwards it to C, node C (two hops away from A down the route) is required to generate acknowledgement packet (TWOACK). When node C sends the TWOACK packet back to A indicates that B has sent packet 1 to C successfully. If A didn't receive TWOACK packet from C within a predefined timeout, then node A marks nodes B and C as malicious nodes

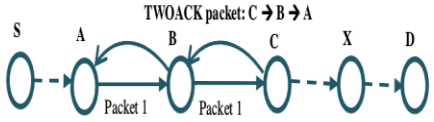

Fig -1 TWOACK Scheme

The Delay per Hop Indicator (DelPHI) [5] introduced by Hon Sun Chiu and King-Shan Lui, can recognize both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find each one available disjoint route between a source and a destination. Then, the delay time and length of each route are calculated and the average delay time per hop along each route is computed. These values are used to recognize wormhole. The route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can identify both kind of wormhole attack; however, it cannot recognize the position of a wormhole. Moreover, because the lengths of the routes are modified by every node, including wormhole nodes, wormhole nodes can change the route length in a certain manner so that they cannot be recognized.

Sun Choi et al. introduced an efficient method called Wormhole Attack Prevention (WAP) without using specific hardware. In WAP All nodes observe its near by node's behavior when they transmit RREQ messages to the destination by using a specific list called Neighbor List. When a sender node receives some RREP messages, it can find a route under wormhole attack among the routes. Once wormhole node is recognized, sender node records them in the Wormhole Node List. Although misbehaving nodes have been ejected from routing in the past, the nodes have a chance of attack once more. Therefore, we store the information of wormhole nodes at the sender node to inhibit them taking part in routing again.

Packet Leash [6] is an approach in which some information in added to restrict the maximum transmission distance of packet. There are two kind of packet leashes: geographic leash and temporal leash. In geographic leash, when a node X transmit a packet to other node Y, the node must include its location information and sending time into the packet. Y can evaluate the distance between X and Y. The geographic leash calculates an upper bound on the distance, while the temporal leash assures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes' clocks is bounded by Δ, and this value should be recognized to all the nodes. Each and every node checks the expiration time in the packet and find out whether or not wormhole attacks have arose. If a packet receiving time exceed the expiration time, the packet is discarded.

Unlike Packet Leash, Capkun et al. [7] introduced SECTOR, which does not need any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). Node X calculates the distance to other node Y in its transmission range by transmitting it a one-bit challenge, which A responds to spontaneously. By using the time of flight, X detects whether Y is a near by node or not. However, this approach uses specific hardware that can reply to a one-bit challenge without any delay as Packet leash.

In order to bypass the problem of using specific hardware, a Round Trip Time (RTT) mechanism is introduced by Jane Zhen and Sampalli. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node X to Route Reply (RREP) message receiving Time from a node Y. X will compute the RTT between X and all its near by nodess. Because the RTT between two false neighbors is higher than between two real neighbors, node X can recognize both the false and real neighbors. In this approach, each node computes the RTT between itself and all its near by nodess. This approach does not need any specific hardware and it is obvious to implement; but it cannot detect exposed attacks because false neighbors are created in exposed attacks.

3. PROBLEM DEFINITION AND PROPOSED SOLUTION

3.1 Problem definition

Several scheme is proposed by researcher to detect intrusion in wirless mobile ad-hoc network but still some need to work in this dimension. One scheme of them is A3ACK, which work in three model. The default model is Aack model which is similar to AACK mode in AACK scheme, where the source node S first sends data packet to destination node D along the active route that is gets from DSR routing protocol. Also, the source node S has to register the sending packet ID and sending time. When destination D receives the sending data packet, it has to generate an Aack packet and sends it back to the source node on the same route path but in opposite direction. If the source node S didn't receive the Aack packet with predefined timeout, it has to switch to Tack model to detect if there is any misbehaving nodes in active route path. The Tack model works similar to TWOACK scheme except that it detects misbehaving nodes instead of links. In Tack model, the third node for every three consecutive nodes in route path has to send back a Tack packet to first node. This process carries out by every three consecutive nodes in a route path. If the source node S fails to receive acknowledgement packet (Tack) within a predefined timeout, it has to switch to Thack model to detect if there are any collaborative misbehaving nodes in the route path. The Thack model aims to solve the problems of receiver collision and limited transmission power and collaborative attacks as well within presence of two consecutive misbehaving nodes in a route path. In the Thack model, every four consecutive nodes in path work together where the fourth node (three hops away from the first one) has to send back an Thack packet to the first node in that group within a predefined time out. The A3ACK scheme is capable to detect two malicious node as well as malicious link in Thack model, but there may be chance to third node is malicious rather than two consecutive nodes. So this scheme is unable to detect third node is malicious or not in four consecutive nodes. Additionally it increase delay of data packets and computation overhead.

3.2 Proposed solution

The inability of A3ACK scheme is sort out by proposing the new enhance scheme. The new enhance sheme keeps track information of ACK packets such as ack for which, from where, ack for whom etc. This characteristics of proposed scheme offers accurate detection of malicous node at third hop with first and second hop. Proposed scheme also decrease computation overhead also.

Table-1 Different intrusion detection schemes

Approach Name	Strength	Weakness	Suitable Application
Wathdog[3]	Watchdog uses to detect malicious nodes in a network that agree to forward packets but fail to do so	It has three Receiver Collision, Limited Transmission Power and CollaborativeAttacks Problems	IDS Implementation
PATHRATER [3]	Pathrater technique uses to bypass these malicious nodes in a route path in the future transmission	Pathrater techniques are able to detect malicious nodes at forward level instead of the lin-k level	Safe Delivery of Data Packets
TWOACK[4]	It solve two of its weaknesses, named, receiver collision and limited transmission power	TWOACK technique is that it generates more overhead and reduces network performance due to acknowledgment every data packet on the route path	Detection of malicious nodes
AACK[8]	Less overhead comparing with TWOACK technique	AACK suffers from detect malicious nodes within the existence of collaborative attacks in a route path	Minimize computation Overhead
A3ACK[9]	It solves three of these six weaknesses, named, receiver collisions, limited transmission power and collaborative malicious nodes in a route path.	A3ACK unable to take decision about malicous node and find exact malicious node	Detection of collaborative attack

4. METHODOLOGY

The entire simulations were carried out using ns 2.35 network simulator [10] which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking. It is advisable for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a collaborative environment. It is distributed as open source software. A large number of institutes and researchers use, maintain and develop NS2. NS2 Versions are available for Linux, Solaris, Windows and Mac OS X.

5. CONCLUSION

Traditional network needs a fixed infrastructure to establish but ad-hoc network has a different approach. Ad-hoc network does not need fix infrastructure. It provides facility to node that they can join or leave network anytime. Ad-hoc network is a very broad area for research due to its wide collection of concepts. Security of MANET is one of the important features for its deployment. The proposed approach tried to identify malicious node into the network. Nodes in the networks which interrupts packet transmission and try to capture transmitted information. In this work we have focused on detection of attack.

6. REFERENCES

[1] Seema Dev Aksatha D, Lalitha T, A Comprehensive Overview on Manet, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3 Issue-6, August 2014

[2] Abdalrazak T. Rahem , H K Sawant, WELL-ORGANIZED AD-HOC ROUTING PROTOCOL BASED ON COLLABORATIVE TRUST-BASED SECURE ROUTING, International Journal of Advances in Engineering & Technology, July 2012.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile ad hoc networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[4] Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137-2142 Vol. 4, 13-17 March 2005.

[5] Chiu, HS; Wong Lui, “DelPHI: wormhole detection mechanism for ad hoc wireless networks”, The 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, 16-18 January 2013

[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", Carnegie Mellon University.

[7] Srdjan Capkun, Levente Buttyan, Jean-Pierre Hubaux, SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks, ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 31, 2003, Washington, USA.

[8] T. Sheltami, A. Al-Roubaiey, E. Shakshuki and A. Mohmoud. Video Transmission Enhancement in existence of malicious Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, 273-282. 2009.

[9] Abdulsalam Basabaaa, Tarek Sheltamia and Elhadi Shakshukib ," Implementation of A3ACKs intrusion detection system under various mobility speeds", 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)

[10] Teerawat Issariyakul , Ekram Hossain, Introduction to Network Simulator NS2, Second Edition , Springer.