ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey Paper on Performance of Intrusion Detection System and Routing Protocols in Wireless Ad-Hoc Network

Jananee V [1] Dhivya S [2] Raghuvaran E [3]

Assistant Professor, Dept. of C.S.E, Rajalakshmi Engineering College, Chennai, Tamilnadu, India [1]

Assistant Professor, Dept. of C.S.E, Rajalakshmi Engineering College, Chennai, Tamilnadu, India [2]

Software Developer, Code Omega IT Services & Consultancy, Chennai, Tamilnadu, India. [3]

ABSTRACT: Mobile Ad-hoc network (MANET) is an essential technology in last decade. MANETs are highly susceptible to attacks due to transportation less and decentralized network. This paper provides an outline of the intrusion detection system (IDS) and protocols by representing their characteristics, functionality and their comparative analysis to evaluate the performance. This study experimentally compares the qualities of intrusion detection system along with the performance of the routing protocols in wireless mobile ad-hoc networks such as AODV, DSDV, ODMR, ZRP and OLSR. This paper concludes that OLSR is to increase the throughput/ bandwidth, to reduce the packet drop and to highly improve the QoS support.

KEYWORDS: Wireless Ad-hoc network, Intrusion Detection System, Optimized routing, Routing protocols

I. INTRODUCTION

In a MANET, the router connection will be moving frequently which will lead to the multiple-hop communication that can permit communication without utilize of Base station (BS)/Access point (AP) and another connections within hotspot cells. A MANET is a movable network so that can change its location, configure itself on the network. All the nodes in the networks will be cellular phone and they use wireless links to communicating. A mobile ad-hoc network is also known as Mobile ad-hoc multiple hop networks without predestined topology. Figure1. A mobile node desires to communicate with correspondent node (CN) via the routers. These nodes associate with their nearest home agent (HA) for identifying the foreign agent (FA). Every agent should be familiar with the status of the mobile nodes. These path routing will be changed dynamically. Some pros of wireless network: they give access to information and service regardless of geographic position. This network can be set-up at any place and time. These networks will able to work without any prearranged infrastructure. Some of the cons of MANETs are: limited resources, physical security and intrinsic mutual trust vulnerable to attacks. Volatile network topology makes it hard to detect spiteful nodes. Most of the Security protocols for wired networks cannot effort for ad hoc networks.

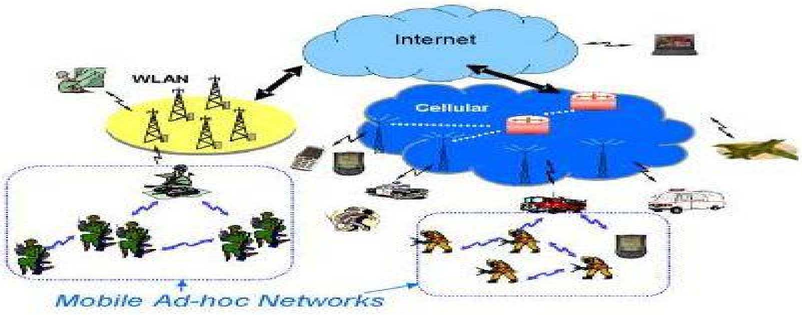

Fig 1. Basic form of Mobile Ad-Hoc Network Architecture

II.RELATED WORK

[6]The mobile nodes that we are focusing our discussion on are current day laptops that have sufficient processing capability and memory to support ad-hoc networking as well as intrusion detection applications. These laptops have limited battery life only when they are unplugged from a main power source. Such nodes are used to setup wireless ad-hoc networks in situations like classrooms or conferences; temporary offices like a promotional booth; emergency search and rescue missions and possibly at command posts in the military.

[4]Mobile Ad hoc Networks are assortment of mobile terminals or nodes, allowing no stationary infrastructure and centralized administration. Several routing protocols have been proposed in recent years for possible deployment of Mobile Ad hoc Networks (MANETs) Ad hoc network is popular nowadays due to the easy disposition and self-configuring nature.

[1]A mobile ad hoc network (MANET) is formed by a group of mobile wireless nodes, each of which functions as a router and agrees to forward packets for others. Many routing protocols (e.g., AODV, DSDV, etc) have been proposed for MANETs. However, most assume that nodes are trustworthy and cooperative. Thus, they are vulnerable to a variety of attacks. Secure routing protocol based on DSDV, namely S-DSDV, in which, a well-behaved node can successfully detect a malicious routing update with any sequence number fraud (larger or smaller) and any distance fraud (shorter, same, or longer) provided no two nodes are in collision. S-DSDV overhead is justified by the enhanced security.

III. INTRUSION DETECTION SYSTEM

[10] Many historical actions have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, these are not enough to solve the issues. As the system become more intricate, there are also more weaknesses, which lead to other security problems. Intrusion detection can be used as a second wall of defense to protect the network from those problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the network.

It can also be differentiated into three categories as follows [10]

1. **Anomaly detection system:** The normal events (normal behaviors) of users are reserved in the system. The system compares the newly captured data with these existing entries and then treats any movement that deviates from the baseline as a possible intrusion action by informing system administrators or initializing a proper query response.
2. **Misuse detection system:** The system keeps signatures of known attacks and uses them to compare with the newly captured activity. If there is any matched, it will consider as an intrusion. Like a virus detection system, it will not find/detect new kind of attacks.
3. **Specification-based detection system:** This system defines a lot of constraints in which describe the proper operation of a program or protocol. Then, it monitors the current execution of the program with respect to the pre-defined constraints.

IV. VARIOUS TYPES OF INTRUSION DETECTION SYSTEM

A. DYNAMIC HIERARCHICAL INTRUSION DETECTION SYSTEM ARCHITECTURE (DHIDS)

Since the entire nodes move randomly across the network, a static hierarchy is not appropriate for such dynamic network topology. Sterne et al. [10] proposed new dynamic intrusion detection hierarchies which will potentially scalable to large networks by using clustering concept. However, it can be controlled in more than two levels as shown in Fig 2. Nodes labeled “11” are the first level cluster heads while nodes labeled “12” are the second level cluster heads and so on. Members of the cluster heads in each level are called leaf nodes.

DOI: 10.15680/IJIRCCE.2016. 0412125

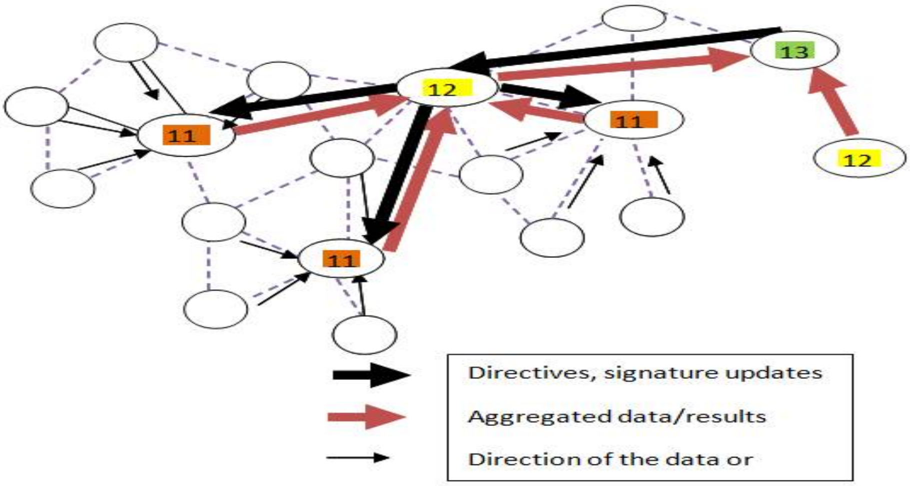

Fig 2. Dynamic Hierarchy Intrusion Detection

Each and Every node has the responsibilities of monitoring (by accumulating counts and statistics), logging and evaluating the data with resulting response to intrusion detected if there is enough evidence and alerting to cluster heads. Cluster heads ought to perform: Data integration and reduction: Cluster heads can be aggregate and associate query reports from every members of the cluster and data of their own. Data reduction may exist to avoid conflict issues, fake data and overlapping reports. Also, cluster heads may send the requests to their children for further information in order to link reports properly.

B. ZONE-BASED NON-OVERLAPPING INTRUSION DETECTION SYSTEM (ZBIDS)

[10] It has planned an anomaly-based non-overlapping Intrusion Detection System (ZBIDS) in two levels. By dividing the network in Fig 3 into non overlapping zones (zone X to zone R), nodes can be classified into two types: intra zone node and inter zone node (or gateway node). Consider only zone V, node 10, 11, 13 and 14 are intra zone nodes, while node 7, 8, 12, and 15 are inter zone nodes which have physical links to nodes in other zones. The configuration and maintenance of zones involve each node to understand its own physical location and to map its location to a zone map, which requires prior design setup environment.

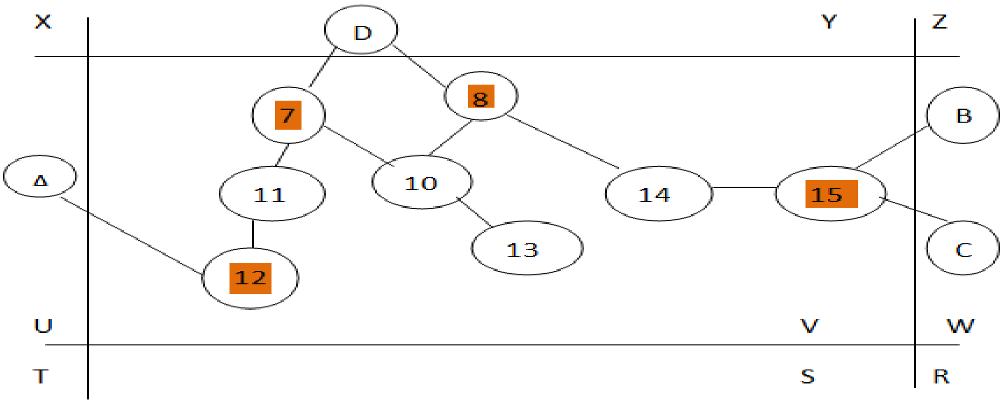

Fig 3. Zone-Based Intrusion Detection Architecture

V. VARIOUS TYPES OF ROUTING PROTOCOLS

A. *AD-HOC ON DEMAND DISTANCE VECTOR (AODV)*

[9] An AODV is one of the routing protocol beneath study by MANET and the distinctive procedure of insist types. In AODV, every node has the routing table and the newness of routes is ensured with the progression number of routing information. When each node receives a manage packet that occur in on-demand, the routing table is rationalized based on the sequence number or the number of hops. If a route to a target is wanted it is recognized at the route discovery stage and is maintained at the route maintenance stage [2]. It constructs route on insist and aims to diminish routing load. It uses a table determined routing construction, target series numbers for routing packets to goal mobile nodes and has place independent algorithm [5]

It performs route detection using organize memo route demand (RREQ) and route answer (RREP), at any time node desires to launch packet to destination. To organize network extensive transmit of RREQs, the base node uses an increasing ring method [4]

When each node receives the RREP, it generates a forward route to the target node and it forwards the RREP to the turnaround route. When the RREP arrives at the base node next to the open route, it updates the forward route and starts relations [2]

B. DESTINATION SEQUENCED DISTANCE VECTOR (DSDV)

In DSDV network maintaining routing tables for every node, which have all the probable destinations and the number of hops to them in the network are recorded. This number is also linked with every route to the goal [4] DSDV is to address the looping difficulty of the predictable expense vector routing protocol and to create the expense vector routing extra apt for ad-hoc networks routing. It arise route rise and fall because of its criteria of route updates. At the same time, it does not answer the general difficulty of every space vector routing protocols, the unidirectional association trouble [1].

Quality of Service Support with DSDV:

(i) Band reservation- It should assign bandwidth at call arrangement time in order to hold up real time connections.
(ii) QoS routing- To hold up QoS for real time traffic, the mobile nodes not only require to recognize the lowest amount wait pathway to target but also have the acquaintance of the BW offered on that path.

C. ZONE ROUTING PROTOCOL (ZRP)

In an ad-hoc network, it can be unspecified that the major part of the traffic is going to seal by nodes. Therefore, ZRP reduces the positive series to a region centered on every node [3]. It takes the benefit of both proactive and immediate protocols. For proactive, it finds inside a node's limited locality Intra zone Routing Protocol (IARP) then by using a immediate protocol for communication between these neighborhoods Inter zone Routing Protocol (IERP). The in charge for the forwarding of a route demand is Broadcast Resolution Protocol (BRP). It divides its network in unlike zone. In this zone there may be several overlapping for every node, with unusual dimension for each node. Radius of extent for every node is given, where perimeter of region for the number of nodes [3]

A Media access control protocols may be used by node to know about the next direct neighbors and also requires a Neighbor Discovery Protocol (NDP) to find the neighbor node in efficient way.

D. OPTIMIZED LINK STATE ROUTING (OLSR)

[6] In Link State Routing, every node occasionally broadcasting position of its relations, and it must re-broadcasts information of connection state received from its neighbor's node. Every node keeps track of that information from further nodes by the use of series information to decide after that hop to each goal. In scenery OLSR protocol is proactive Protocol. Purpose is to route immediately available and minimizes the flooding by using Multi Point Relay (MPR). [8] For large and dense networks OLSR protocol is suitable. Routing table has been maintained for each node to know its target node in the network. Every node getting Topology Control (TC) message after that it will store connected pairs of outline (last-hop, node). Maintain routing table based on the information carried in the topology

table and the neighbor table and also it contains unique ID for every node, destination address, after that hop address and distance [11].

Protocol	DSDV	AODV	ZRP	OLSR
Unicast routes	No	No	Yes	Yes
Multicast routes	No	Yes	No	Yes
Periodic broadcast	Yes	Yes	No	Yes
Distributed	Yes	Yes	Yes	Yes
Unidirectional link support	No	No	Yes	Yes
Jitter	High	High	High	Low
QoS Support	No	No	No	Yes

Table 1.Comparison table of routing protocols [7]

VI. CONCLUSION

In this paper, we have analyzed the Intrusion Detection System (IDS) with Dynamic Hierarchical Intrusion Detection system (DHIDS), Zone-Based Intrusion Detection System (ZBIDS) and presentation contrast of the routing protocols in ad-hoc network. In wireless ad-hoc network there is no QoS hold up in space vector and hybrid routing protocols. An effort has been prepared to focus on QoS in optimized link state routing protocol. Moreover, study consequence shows that OLSR protocol can be bared to raise the throughput and reduce the packet drop.

REFERENCES

[1] Guoyou He"Destination-Sequenced Distance Vector (DSDV) Protocol", *Networking Laboratory,Helsinki University of Technology*.

[2] Abolfazl Akbari, Mehdi soruri and Ali Khosrozadeh "A New AODV Routing Protocol in Mobile Adhoc Networks, ,Islamic *Azad University Ayatollah Amoli Branch, Amol, Iran Islamic Azad University Science and Research Branch, Tehran, Iran World Appl. Sci. J.*, 19 (4): 478-485, 2012.

[3] Nicklas Beijar, "Zone Routing Protocol (ZRP)" *Networking Laboratory, Helsinki University of Technology*,P.O. Box 3000, FIN-02015 HUT, Finland.

[4] Ginni tonk, indu kashyap,s,s.tyagi, "Performance comparison of ad-hoc network routing protocols using ns-2.

[5] Thakare p.p, joshi M.A. and Raut A.D "A review paper on routing protocols of wireless ad-hoc network technology",.,Department Of Computer Science, *Jawaharlal Darda Institute Of Engineering and Technology, Yavatmal ,Ms,India,International Journal Of Networking*, Issn:2249-278x & -Issn: 2249-2798, Volume 2, Issue 1, 2012.

[6] Qamar Abbas Tarar, Optimized Link State Routing Protocol for Ad Hoc Networks "Mobile ad-hoc networks based on wireless LAN".

[7] S.A .Ade , P. A. Tijare, "Pertformance comparision of AODV, DSDV, OLSR and DSR Routing protocols in Mobile Ad Hoc Networks, *International Journal of Information technology and Knowledge Management July-December 2010*, Volume 2, No. 2, pp. 545-548.

[8] Prof. Robert W. Health Jr. "Wireless Networking and communication Group".

[9] Ali Khosrozadeh, Abolfazle Akbari, Maryam Bagheri and Neda Beikmahdavi, "A New Algorithm AODV Routing Protocol in Mobile ADHOC Networks" Department of Computer Engineering, Ayatollah Amoli Branch Islamic Azad University,Amol,Iran, *International Journal of Latest Trends in Computing IJLTC*, E-ISSN: 2045-5364, Vol-2 No 3 September, 2011.

[10] Tiranuch Anantvalee , Jie Wu . "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Wireless/Mobile Network Security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 170 - 196 c °2006 Springer

[11] Raghuvaran E , "A Survey Paper on Performance of Routing Protocols in Wireless Ad-Hoc Network" , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 770-773

BIOGRAPHY

Mrs. Jananee V[1], M.E., Working as Assistant Professor (SS) in the Department of Computer Science at Rajalakshmi Engineering College, Chennai. Her area of interest is Wireless Mobile Ad Hoc Networks.

Ms. Dhivya S[2], M.E., Working as Assistant Professor in the Department of Computer Science at Rajalakshmi Engineering College, Chennai. Her area of interest is Wireless Mobile Ad Hoc Networks.

Mr. Raghuvaran E[3], M.E., Working as Software Developer in Code Omega (IT Services & Consultancy, Chennai). His area of interest is Wireless Mobile Ad Hoc Networks.

DOI: 10.15680/IJIRCCE.2016. 0412125