International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Routing Protocols & Intrusion Detection Techniques over MANET: A Survey

Preeti Pandey[1], **Atul Barve**[2]

[1]Mtech Student, Oriental Institute of Science and Technology, Bhopal-462022, India

[2]Associate Professor, Oriental Institute of Science and Technology, Bhopal-462022, India

Abstract: ***The main feature that distinguishes the network from malicious wireless network or wired is another mobility and density of the contract. A mobile ad-hoc network (MANET) is a network which is infrastructure less, each node play role of transmitter and receiver data router. Therefore, it has been MANET routing to adapt to the dynamic changes in topology protocols design, while maximizing performance and packet delivery ratio and reduce the delay adds a good start, the anger of the average and minimum packet loss. Current performance of MANET routing protocols on mobility and density factors decade. Results vary when we change the density of the node. This article also provides a survey of the many schemes available intrusion detection dedicated networks. We also described some of the basic attacks in ad hoc network and discuss solutions available***.

Keywords: AODV, DSR, DYMO, IDS, MANET, OLSR and ZRP.

1. Introduction

In recent years, wireless networks such as multihop ad hoc networks, sensor networks and the car is very important subject of research. A MANET is a form of a network which configure by itself. MANETS are mobile and use wireless connections to connect to various networks without any fixed infrastructure or centralized management system. In recent years, MANET continues to attract interest in various fields. In order to ensure the efficient operation with a total contract MANET becomes too large, it must overhead routing algorithms to be low, independent of the total number of contract employees in MANET. Mobility, density knots and the lack of any fixed infrastructure make it very attractive for mobility operations MANET applications rescue embarrassment and time. Because the contract are free to move randomly, and network topology can change rapidly and can be unpredictable, which makes the traditional protocol unsuitable in MANET. It effects the ongoing transmission Mobility, since the mobile node that receives and sends packets may not be in the range. Featuring decade the movement pattern of MANET mobility models and each routing protocol has specific characteristics of these models. In order to find more adaptive and efficient routing topology dynamic MANET protocol, you must analyze the behavior of routing protocols at different speeds of the decade, the number of traffic nodes, network size and density of the contract. Challenges include MANET required: not reliable wireless connections between nodes, dynamic topology, the lack of secure borders and threats of the contract involved in the network, not to ease the central management, supply restricted the power and scalability [1]. Security issues are also there as the attacks, session hijacking, eavesdropping, jamming, denial of service etc. [2].

The above discussion leads us to believe that it is the first to understand and evaluate the performance of routing protocol in different scenarios for mobility before choosing a protocol for that scenario. Most of the previous studies with the mobility routing protocols select random waypoint for the simulation model. This paper presents the results of a number of proactive, interactive and hybrid protocols such as customized demand vector (AODV) routing Dynamic source (DSR), and dynamic demand MANET (Demo) State routing optimal link (OLSR) and the routing protocol (ZRP). Performance analysis of performance measures is limited.

2. Routing Protocols on MANET

The routing protocols in MANET are IP based. It uses unicast, multicast or hybrid techniques and also interacts with standard wired IP services rather than being regarded as a complete separate entity. Figure 1 shows the categorization of different types of routing protocols in MANET.

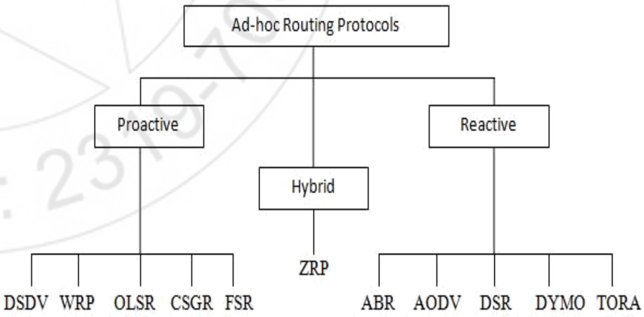

Figure 1: Categorization of Routing Protocols in MANET

2.1 Reactive Routing Protocols

This protocols (also known as demand-based), and discovered a path only when necessary. Nodes maintain rode to active destination. It is reduced communications costs on account delay due to discuss the way. These protocols are great dedicated to the environment to be saved on battery power by not sending both announcements receiving any [3]. All nodes discovered to maintain the roads in their routing tables. However, only preserving the correct paths and roads are deleted after the previous deadline of active way. And created a serious problem when the network reaches from spam bots failures occur due to high mobility of the node. At the same time, new links between remote nodes can be set previously. This dramatically increases network traffic related to the impact of emissions / fast intermediate nodes link password. Figure 2 shows the process of discovering the way for interactive routing protocol [4].

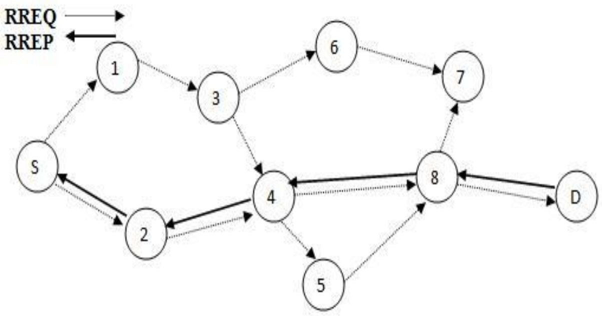

Figure 2: Route Discovery Process

2.1.1 Ad-hoc on Demand Distance Vector (AODV)

Custom application protocol vector-distance and interactive way should only require a road when you need one and does not require mobile contract maintains the roads to destinations that do not communicate. AODV ensures a loop involving the use of sequence numbers indicate how new ways or new on the road. AODV requires that each node maintains a routing table containing the entry route for each destination node, which is communicated. Each entry road to follow some areas, such as the IP destination address, destination sequence number, the next hop count. Find your way to a destination, a node using the package emits a request AODV path (RREQ). It Contains RREQ IP address of the node, and the current sequence number, ID number and deployment of the latest known point of the aircraft to the sequence of the source node. Destination to receive RREQ node, the group unites and respond the way (RREP) along the reverse path established in the contract during the intermediate route discovery process. In the event of a link failure, it sends the wrong road package (RERR) to the decade of origin and destination. Using the sequence numbers, the source nodes is always able to find new ways valid [5], [6].

2.1.2 Dynamic Source Routing (DSR)

Such as AODV, DSR puts the road to the destination at the request of the source node. DSR uses source routing strategy. In source routing, the source must know the sequence of the target node. Each node maintains a cache of the road, where they are all known ways to store. Route discovery process begins, but if you cannot find the desired path in the cache road. To limit the number of requests for dissemination methods, the node processes the request through message only if you were not already received a letter and address is not in the path log message. DSR uses source routing, which determines the source of full-hopping sequence of each packet path must go. This requires that the movement sequence is included in the header of each packet. The result is negative so it is overhead for routing each packet to carry. However, the great advantage is that intermediate nodes can learn ways to route back to the packages they receive. Since find any way are usually expensive in terms of time and bandwidth, energy, process, and this is a strong argument for the use of the argument source routing. Another advantage to guide the source is that it avoids the need to guide the updated information in the Mediterranean included in the packages. Finally, avoid routing loops that are easily specifying the full path from one node instead of a decision by hip-hop [7].

2.1.3 Dynamic MANET on Demand (DYMO)

DYMO routing protocol multi-hop mono allows interactive routing between routers demo participants. The basic function of the DYMO protocol is the discovery of route and maintenance of roads. During the discovery of the way, the router DYMO initiator spread RREQ network processing begins to find a route to the router DYMO goal. During this process, the deployment of B-Hip-Hop, DYMO receives each router and intermediate in the RREQ, responds with sending RREP hop by hop to the originator. When the initiator receives DYMO RREP routing device, you can select routes between the router sources routing DYMO, the goal in both directions [8]. In order to respond to changes in the decade of the network topology maintains the roads and watches your prayers, when a data packet to a path or a link that is no longer available for the source of the package is to receive notification. Wrong track is sent (RERR) to the package source to indicate that the current path is broken. Once the source has RERR, you can perform the discovery of the way if you still have to deliver packages [9].

2.2 Proactive Routing Protocols

In proactive schemes, the approximations are based on the tables; each node maintains complete constantly routing information of network. When a node needs to redirect the package from affordable root, it searches the route from the table. Therefore there is no delay in finding the root. However, the topology is very dynamic and proactive plans to spend a considerable amount of scarce resources Wireless to maintain full routing information correctly [10]. The proactive routing protocols need to update the routing table when the nodes alter in high frequency. It reduces the performance of the network.

2.2.1 Optimized Link state Routing (OLSR)

It follows three mechanisms for routing; (a) periodic HELLO messages for neighbor sensing. (b) Control packet flooding using Multi-Point Relay (MPR) and (c) path selection using shortest path first algorithm. Each node, by using its two-hop neighbors is accessible. Nodes then rebroadcast only those messages that are received from nodes who selected it as an MPR. This mechanism efficiently reduces the broadcast control overhead and thus each node has a partial topology graph of the whole network. Each node is selected as an MPR and transmits Topology Control (TC) messages to broadcast the presence of it to the MPR selector set. TC messages contain originating nodes address and its MPR selector set. Once routes are available to source node, it selects the optimal path using shortest path first algorithm [11].

2.3 Hybrid Routing Protocols

It is the third category of routing schemes in MANET, which has proactive and reactive, both approaches in combined form. Zone Routing Protocol is a type of hybrid protocol.

2.3.1 Zone Routing Protocol

This Routing Protocol implies both pro-active and re-active hybrid approach. It is the hybrid scheme, which follows the proactive detection of a node's neighborhood and applies the reactive protocol approach for communication between these two neighborhood nodes. These proactive and reactive approaches implementing the routing protocols for MANET has some disadvantages. ZRP provides a framework for different protocols. It separates the local neighborhood nodes from the global topology for the entire network. Thus allows following different approaches. The local nodes are called zones. Each node may be within multiple zones. The size of zone may be dissimilar. It is identified by a radius of length L, here L is the node count in a zone. Figure 3 shows the routing zones of L=2.

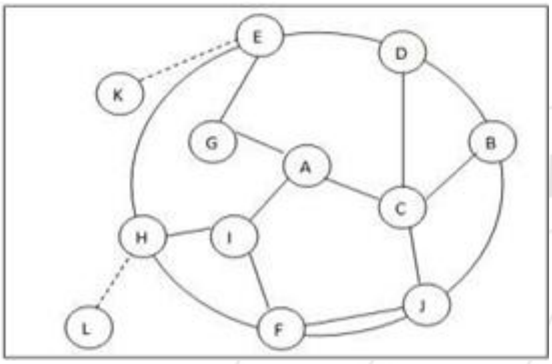

Figure 3: Routing Zone of node A with L=2

3. Intrusion Detection System

Intrusion detection systems have become (IDS) the most important part of security. IDS are very essential part of a comprehensive system for information security component. Intrusion detection is to monitor computer systems or networks from unauthorized access or activity or modify files process. It can also be used IDS to monitor network traffic, so you can detect the system in case of being attacked by a network attack, attack from the black hole, or denied service attack. The intrusion detection system can also be defined as the disclosure of which is automated system type which is used to alert the security management system available and generate alarm in place of the attack. If there are any attacks or interventions or something different from the normal activity, IDS come into existence and took action. IDS revealed achieved through continuous monitoring and analysis of network activity is normal, some of the special attacks and activity is not the same everyday [2.3] activity.

3.1 Types of IDS

IDS can be classified into two types- depending on data collection mechanism and detection techniques. The IDS based on the data collection method thus categories into two- Network based IDS and Host based IDS. Network-based IDS executes on the gateway of a network or on a router. It captures and also monitors the network traffic that goes through it. It will be useful to detect attack from outside. This is not suitable for MANET since there is no central coordination. A host-based IDS captures local network traffic of a specific host. It is better for detecting attack from inside. While on the other hand, there are mainly three types of IDS that comes under the category of detection techniques [4], are as follows-

3.1.1 Anomaly Detection System

In this type of detection system the normal behavior or daily activities of a user are keeping inside the system. Whenever any activity is performed by the user or attacker, the system compares this activity with the kept data, and then treats that activity based on the evaluation, whether it is an intrusive activity or not, and respond to the system.

3.1.2 Misuse Detection System

In the misuse detection system, it holds some well known attack's pattern and their signature. Whenever any activity is performed, it compares this activity with stored pattern or signature and if any match is found then it treated as an intrusive activity. We can take virus detection system as an example of this type. But the main drawback of this system is that it can't identify new types of attack [2].

3.1.3 Specification Based Detection System

This type of system defines a set of rules and describes the procedure of a program or protocol. Whenever any activity is performed, it checks the execution of that activity with defined set of rules

4. Intrusion Detection in MANET

Intrusion is an activity through which the integrity, confidentiality, or availability of information is altered. Intrusion detection system (IDS) is a system or application software that monitors network traffic and if it detects any, and then alert the director of suspicious activity system or network. [5]. Have been many systems proposal intrusion detection for wired networks in which all traffic passes through the switches, routers or gateway for IDS can easily be implemented on these devices. While on the other side MANET does not have all these devices and any user can access it because of the open environment. Therefore, the current technology in IDS wired network cannot be implemented directly in MANET. There are basically three types of techniques IDS [6], which can be applied in MANET

4.1 Stand Alone Intrusion Detection System

In this system, the intrusion detection system runs independently on the individual node to determine infiltration. Any decision on a specific activity based solely on the information gathered on its own knots, because there is no cooperation between network nodes. Therefore, the transfer of any information even the same node network has no information on other network nodes, where the transfer of any warning information. This model is not effective because of his palaces, and can be applied effectively in the network where all nodes already have installed IDS. This system is also suitable for single-layer network compared with the multi-network infrastructure layers. Because the information available on one node is not sufficient to detect intrusions, it is not selected this system as IDS network from intruders.

4.2 Distributed and Cooperative Intrusion Detection System

In this architecture, each node agent IDS detects intrusions locally and cooperate with neighboring nodes to detect the world provided that the evidence available is not specified and required a broader search. Whenever been arrested infiltration, agent IDS may issue a local response (for example, alert the local user) or a global response. Each node involved in the infiltration detection and response way agent IDS in which it operates. Responsibility agent IDS is to detect and gather information and local data to determine any attack if there is any attack on the network, and also take a solution independently. However, the neighboring IDS agents also assist in discovering the global offside when the data is uncertain. IDS are an independent and this system is also suitable for the flat network system, not for multi-layer system.

4.3 Hierarchical Intrusion Detection System

HIDS extends the capabilities of IDS hierarchical IDS system of distribution and collaborative been implemented for infrastructure and multiple layers of the network where the network is divided into different networks known as small groups. Every president bloc usually has more functionality compared with other members of the cluster, and the movement of data packets to other groups. So, we can say that these presidents cluster, one way or another, do their work as a central point, which is similar to wired control network devices such as routers, switches or phrase. The concept of multi-layer systems applied to intrusion detection by IDS proposed hierarchical. Each agent IDS operates on a node certain member who is responsible for her knots, no screens and decide on locally detects intrusions. The head of the group is responsible for a node locally and globally for the group, such as a network monitor and publicize the passage of the global response to the movement when it was revealed to infiltrate the network.

5. Conclusion

Ad hoc networks are a promising area of research is increasingly with many practical applications. However, the network of hackers is vulnerable to attack, due to changes in the structure, and the lack of infrastructure and the opening of a vital means of a central connection. Because of this weakness and ways to prevent infiltration, such as authentication and encryption are not able to eliminate the attacks, but only reduces attacks. Intrusion detection system (IDS) is one of the most active research areas in MANET it has suggested many authors on their identity by using different techniques.

References

[1] Zaiba Ishrat, ”Security issues, challenges & solution in MANET”, IJCST Vol. 2, Issue 4, pp. 108-112, Oct . - Dec. 2011.

[2] Priyanka Goyal, Vinti Parmar, Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM, Vol. 11, pp. 32-37, January 2011.

[3] Adam N., Ismail M. Y., Abdullah J., Effect of node density on performances of three MANET routing protocols, ICEDSA, Pages: 321-325, 2010.

[4] Sakar N. I. Lol W.G., A study of MANET routing protocols: Joint node density, packet length and mobility, ISCC, Pages: 515-520, 2010.

[5] B.A.S Roopa Devi, Dr. J. V. R Murthy, Dr. G. Narasimha,” Impact of Different Mobility Models on AODV Protocol in MANET with NS-2.35 and Bonnmotion-2.1a”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 10, pp. 827-8231, October 2014.

[6] [6]Pandya M. And Shrivastva A.K., Improvising the performance with security of AODV routing protocol in MANETs, NUiCONE, Pages: 1-6, 2013.

[7] Barati M., Atefi K., Khosravi F. And Daftri Y.A., Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET, ICCIS, Pages: 636-642, 2012.

[8] Wasiq S., Arshad W., Javaid N., Bibi A., “Performance evaluation of DSDV, OLSR and DYMO using 802.11 and 802.11 lip MAC-protocols”, Multitopic Conference (INMIC), 2011 IEEE 14th International, Pages: 357 - 361, 2011.

[9] Sagar, S.; Saqib, J.; Bibi, A.; Javaid, N.,” Evaluating and comparing the performance of DYMO and OLSR in MANETs and in VANETs”,Multitopic Conference (INMIC), 2011 IEEE 14th International”, Pages: 362 - 366, 2011.

[10] Kumar D., Srivastava A. And Gupta S.C., Performance comparison of pro-active and reactive routing protocols for MANET, ICCCA, Pages: 1-4, 2012.

[11] Kumar, S.; Javaid, N.; Yousuf, Z.; Kumar, H.; Khan, Z.A.; Bibi, A.,” DSDV, DYMO, OLSR: Link Duration and Path Stability”, Trust, Security and Privacy in Computing and Communications (TrustCom), Pages: 1862 - 1866, 2012.

[12] Ravilla D. and Putta C.S.R., Performance of secured zone routing protocol due to the effect of malicious nodes in MANETs, ICCCNT, Pages: 1-8, 2013.

[13] GS Tomar, Laxmi Shrivastava, SS Bhadauria, “Load Balanced Congestion Adaptive Routing for Randomly Distributed Mobile Adhoc Networks”, Springers International Journal of Wireless Personal Communication, Vol.75, No.2(II), pp 2723-2733, Feb 2014.

[14] Laxmi Shrivastava, SS. Bhadauria, G.S. Tomar, "Influence of Traffic Load on the performance of AODV, DSR and DSDV in MANET", International Journal of Communication Systems and Network Technologies, Vol.1 Issue 1. pp 22-34, Apr 2013.