Intrusion Response System in AODV for MANET

Manoj Kumar
M.Tech., Research scholar,
Department of Computer Science &
Engg., GNDEC, Ludhiana,India

Akshay Girdhar
Associate Prof., Department of
Information Technology, GNDEC,
Ludhiana, India

ABSTRACT

The mobile adhoc network (MANET) requires effective intrusion response system. In this paper, we present an intrusion response system that supports the infrastructureless nature of MANETs. We propose a NHELLO and Link Layer based solution towards excluding malicious node which is robust against address spoofing from the attacker. In particular, we investigate how power adaption can be used to keep a malicious node away from normal node's transmission range. Important issue in this strategy is to select optimal transmission power so that malicious node goes out of operating zone of network, as well as node adapting power itself remains in the operating zone. We also provide a detailed performance evaluation based on various network parameters i.e. a series of simulation studies. Our results show that the proposed concept significantly improves the overall security of mobile ad hoc network without having geographical information of nodes.

General Terms

Computer Network; Wireless; MANET, Security

Keywords

Keywords -Blackhole Attack, IRS, IDS, Power adaption

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an infrastructureless, multi-hop network, in which mobile nodes communicate directly and cooperatively with each other. As there are no access points or routers, no coordination or configuration prior to setup of a MANET is required [3], it is very difficult to centralize administration on MANET in different issues such as routing, authentication, or congestion control. Also, due to high mobility, resource constrains (power, storage, and bandwidth) in MANET environment, and nodes operating in a dynamic topology, more challenges are encountered in routing.

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol i.e. the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors [11].

A variety of attacks are possible in MANET. Some attacks apply to general network, some apply to wireless network and some are specific to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in MANET and all other networks can be roughly classified by the following criteria: passive or active, internal or external, stealthy or non-stealthy, cryptography or non-cryptography, different protocol layer related [2]. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV

Since it is not our goal to develop a new IDS approach for MANETs, our IDS is ample to provide a reasonable detection performance of our implementation of the black hole attack. We mainly concentrated on IRS technique for MANET. We adjusted the parameters so that the IDS achieve a performance that is comparable to that of other systems proposed in literature

2. RELATED WORK

Related work that has motivated and influenced our research can be found an Intrusion System in AODV in MANET and among application domains for adaptive transmission power.

2.1 Approaches in MANETs

Several routing mechanisms for MANETs that take into account geographical information of nodes have been proposed. An overview can be found in [10]. Two of these protocols which are related to our work are LAR [17] and DREAM [13]. Both protocols use location information to restrict the propagation of broadcast messages as it is done in *GeoSec*. A precondition for LAR and DREAM is that the nodes are aware of their geographical position. One way to determine this would be the use of GPS [6]. Besides this, other approaches for the determination of positions in dynamic environments have been proposed. A survey can be found in [1]. The localization mechanisms presented there were developed for sensor networks but can also be applied to mobile ad hoc networks. The approaches can be categorized according to whether the outcome is a global unique position or a position relative to a specific local neighbor. Our approach neither requires globally available information nor global unique positioning. We proposed an intrusion response system i.e. based on NHELLO [8], Link Layer feedback and power adaptive transmission.

2.2 Power Adaptive transmission

Adaptive transmission power has a wide range of applications in wireless networks. Saving battery power or signal strength control for CDMA based systems are prominent examples. In MANETs, adaptive transmission power is mainly used for controlling and optimizing the network topology. One of the first approaches of power aware routing in MANETs is proposed in [15]. Metrics for optimal routing with respect to energy consumed are specified and validated by simulation. Distributed heuristics for topology control without the necessity to exchange additional control information are proposed in [12]. A distributed protocol for topology control in order to achieve a connected network by adapting transmission power such that an optimal number of neighbors per node is maintained, is proposed in [4]. In contrast to [4], control messages are needed. Algorithms for adaptive network-global as well as individual transmission power in MANETs with the goal to achieve a maximized throughput (not minimal energy) subject to the network load and the network density (nodes per area) have been proposed in [14]. No additional messages are needed, but for individual transmission power the 802.11 protocol is extended to prevent asymmetry. A protocol for maximizing network lifetime by adaptive transmission power on a per-node basis has been proposed in [7]. The algorithm works in a distributed way and for this requires the exchange of corresponding protocol messages. To the best of our knowledge, no related work exists that utilizes an adaptive transmission power in the context to keep away the malicious node.

2.3 NHello Message & Link Layer Feedback

Local Repair is only initiated when a link breaks in an active route because a node is not locally connected. So each node must have an immediate and accurate knowledge about the connectivity to its neighbors. The main methods used by AODV to detect the local connectivity to a neighbor are link layer feedback and NHello message [16]. Link layer feedback is a passive method to detect the connectivity. It can quickly identify the link failure during transmission of a data packet to another node. But it needs the support of the underlying MAC protocol. In contrast to link layer feedback, NHello message is an active approach. It requires periodic locally broadcast messages that are utilized to indicate the link availability. Each and every node broadcast Nhello messages every HELLO_INTERVAL to indicate its availability. Once a link is established, failure to receive a NHello message for ALLOW_HELLO_LOSS * HELLO_INTERVAL time from a neighbor indicates a loss of connectivity to that neighbor. This method has a long latency to detect the loss of connectivity to a neighbor. Furthermore the periodical broadcast increases the overhead of the network. However, it has its own advantages. As an active approach, the NHello message mechanism is simple to implement. It can be easily applied to different kinds of networks without any requirement on the underlying implementation. In IRSAM, both link layer feedback and NHello message approaches are used to implement Intrusion response system for MANET.

3. ARCHITECTURE

3.1 The Blackhole Attack

To obtain a worst-case misbehavior, we focus on an aggressive version of the black hole attack that has a devastating effect on network performance. A black hole attracts any communication which is, subsequently, dropped instead of being forwarded to the actual receiver. This is achieved by pretending attractive routes towards destination. The attractiveness of routes is defined by their length (hops) and their age. Therefore, the black hole claims that the destination intended is its direct neighbor. Additionally, the routes offered by the black hole appear to be newer than routes offered by the destination. This way, the route offered by the black hole will be preferred by AODV. We implemented the black hole behavior for the routing protocol AODV which we utilize in our work.

3.2 Intrusion Detection System

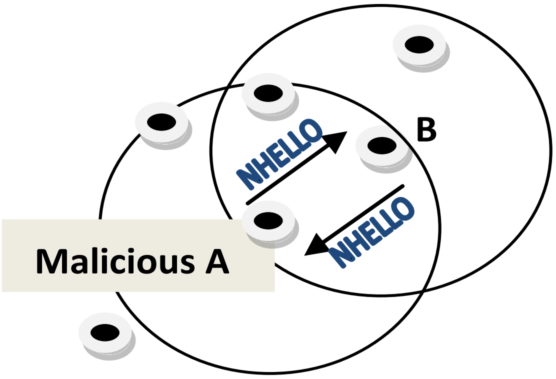
Intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource [5]. Intrusion protection techniques works as the first line of defense. However, intrusion protection alone is not sufficient since there is no perfect security in any system, especially in the field of ad hoc networking due to its fundamental vulnerabilities. Therefore, intrusion detection can work as the second line of protection to capture audit data and perform traffic analysis to detect whether the network or a specific node is under attack [18]. Once an intrusion has been detected in an early stage, measures can be taken to minimize the damages or even gather evidence to inform other legitimate nodes for the intruder and countermeasures maybe launched to minimize the effect of the active attacks.

An intrusion detection system (IDS) can be classified as network-based or host-based according to the audit data that is used. Generally, a network-based IDS runs on a gateway of a network and captures and examines the network traffic that flows through it. Obviously this approach is not suitable for ad hoc networks since there is no central point that allows monitoring of the whole network. A host-based IDS relies on capturing local network traffic to the specific host. This data is analyzed and processed locally to the host and is used either to secure the activities of this host, or to notify another participating node for the malicious action of the node that performs the attack.

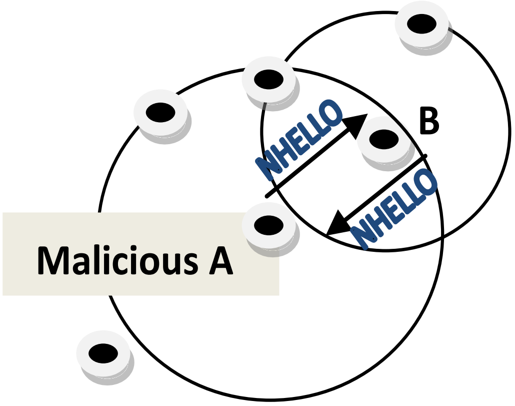
In our IRSAM, we utilize an IDS i.e. used to detect the Blackhole attack in MANET. Each node in MANET operates in Permissious mode to keep track of packets sent and received by its neighbors. Every node uses its packet ratio (sent packets/received packets) to determine Blackhole node in the MANET. If the threshold value (sent packets equal to received packets/2) is greater than packet ratio then declare node is Blackhole node.

4. IRSAM CONCEPTS

All The basic concept of Intrusion Response System for AODV in MANET (IRSAM) is to recover MANET from various security attacks. Figure (a) and (b) briefly explain the concept of IRSAM.



(a) : Node B & Malicious node A in their Transmission Ranges



(b) : Malicious node A out of Transmission Range

It shows oval shape nodes in Adhoc network, node A is assumed as a malicious node. IDS operating in all neighboring nodes of A (for ex. node B) detects it as a malicious node by checking certain parameters of hop count & traffic going in or out etc. After detecting node A as malicious node, all neighboring nodes decrease their transmission power so that node A goes out of their range and is not able to listen to their traffic as shown in figure (b). Node A will be out of the operating zone of the network, and will not be able to affect the performance of MANET.

Important issue in this strategy is to select optimal transmission power so that malicious node is out of operating zone of network, as well as node adapting power itself remain in the operating zone. As discussed in [6], it utilizes geographical position of nodes to calculate optimal transmission power. The IRSAM utilizes NHELLO [8] message an extension of HELLO message for performing this task. NHELLO message carries neighbor information of nodes & is continuously broadcast for link connectivity information. Node B will continuously receive NHELLO packet from A containing itself as neighbor node. After it decreases its power and goes out of A's range, A will not have B in its neighbor list and will not appear in NHELLO packet. So, NHELLO will act as a signal to B for selecting an optimal transmission power.

5. RESULT AND DISCUSSION

5.1 Parameters Chosen for Evaluation

It is necessary to choose suitable metrics for evaluation intrusion response system protocol. The performance metrics describes the outcome of the simulation or set of simulations. These metrics are interesting because they can be used to point out what really happened during the simulation and provide valuable information about the response system protocols. The following metrics are chosen in this work for evaluation of IRSAM having comparison with classic AODV, having two scenarios corresponding to variations in pause time and speed of nodes participating in MANET.

5.1.1 Packet delivery ratio

The ratio between the number of packets originated by the application layer at CBR source and the number of packets received by application layer at CBR sink at final destination. It is desirable that a routing protocol keeps this ratio high. The greater this ratio is, the reliable the adhoc network will be.

Packet Delivery Ratio = Received packets / Sent packets

Packet delivery ratio is important as it describes the loss rate that will be seen by the transport protocols, which in turn affects the maximum throughput that the network can support. This metric characterizes both the completeness and correctness of the routing protocol. The IRSAM has more packet delivery ratio as compare to classic AODV for both scenarios as shown in graphs of figure 3 and figure 9.

5.1.2 Routing Overhead

The total number of routing packets transmitted & received by all the nodes during the simulation known as routing overhead as energy dissipates both in sending a packet as well as receiving a packet for processing it. For packets sent over multiple hops, each transmission of the packet counts as one. This is interesting metric. In some way it reveals how bandwidth efficient the routing protocol is. The routing overhead metric simply shows how much of the bandwidth (which often is one of the limited factors in a wireless system) that is consumed by routing messages, i.e. the amount of bandwidth available to data packets. The routing overhead is typically much larger for proactive protocols since it periodically floods the network with updates messages. As the mobility in the network increases, reactive protocols will of course have to send more and more routing messages. This is where the real strengths and weaknesses of the routing protocol revealed. It is an important metric for comparing protocols, as it measures the scalability of a protocol, the degree to which it will function in congested or low-bandwidth environments. The graphs in figure 1 and figure 7 show that, the IRSAM has less routing overhead as compared to Classic AODV.

5.1.3 End-to-End Delay

End-to-End Delay is average time a packet takes for delivery to its destination after it was transmitted. It tells how a protocol adapts or arranges for an immediate delivery of packets to its desired destination. Average delay is caused by

- Route Discovery Latency
- Queuing at the interface queue

- Retransmission delays at the MAC
- Propagation delay
- Transfer time

The Simulation is used for comparative study of the efficiencies of the AODV and IRSAM. The Graphs of figure 2 and figure 8 shows end to end delay behavior for both Scenarios (Pause Time Variations and Speed Variations). The Graphs shows that the IRSAM has less end to end delay time as compare to classic AODV.

5.1.4 Maximum Packet Sent

The Maximum Packet sent metric is used to determine number of data packets delivered to the destination in a networks as the Graphs shown in figure 4 and figure 10 of both scenarios (Pause Time Variations and Speed Variations), more data packets are sent in IRSAM than Classic AODV. The IRSAM provides more flexibility for data packets transmission in MANET.

5.1.5 Maximum Packet dropped

The maximum packet dropped parameter determines total numbers of data packets lost during transmission in the network. The classic AODV dropped more packets as compare to our purposed IRSAM concepts as graphs shown in figure 5 and figure 11 for both scenarios (Pause Time Variations and Speed Variations).

5.1.6 Hello Load

The hello Load metric describes the number of hello load packets used during packet transmission in MANET those are used periodically to check the connectivity of nodes in MANET. The hello packets also increase the load of network. As graphs shown in the figure 6 and figure 12 for both scenarios (Pause Time Variations and Speed Variations)

5.1.7 Simulation Parameters

Various default parameters like Channel, Propagation medium, Network Interface type, MAC protocol, Link layer type, interface queue, antenna type are same for both scenarios. Other default parameters like path of node-movement file and traffic-generation file are needed to mention accordingly in the tcl script file. The simulation parameters used to produce the simulation suite for this work are presented and explained as follows:

A scenario size is chosen as 1000m x 1000 m square because square area does not discriminate one direction of motion like rectangular area do. The transmitter range of IEEE 802.11 nodes in ns-2 is 250m [9] and this is maximum possible distance between two mobile nodes. They cannot communicate with each other beyond this. The source-destination pairs are spread randomly over the network. The number of source-destination pairs and the packet sending rate in each pair is varied to change the offered load in the network. Traffic sources are CBR (continuous bit-rate). Each node starts its journey from a random location to a random destination according to the speed parameter specified in the scenarios. Once the destination is reached, another random destination is targeted after specified pause. Simulations are run for 100 simulated seconds for 50 nodes. For fairness, identical mobility and traffic scenarios are used across protocols. All the simulation parameters are summarized below in table 1

Table 1: Summary of common Parameter used in Simulation

Parameters	**Value**
Transmitter Range	250 m
Bandwidth	2Mbits/s
Simulation Time	200
Number of nodes	50
Scenario size	1000 x 1000 m2
Traffic type	Constant Bit Rate
Packet size	64 bytes
Flows	25
Rate	4 packets/s

5.2 Senario-1: Pause Time Variation

In Scenario-1 protocols are tested in 6 different pause time levels 0, 20, 40, 60, 80, 100 with speed varies from 1-20m/s. Rest of the parameter remains constant. Following sections discusses results after simulation in terms of six routing parameters of MANET- routing overhead, average end to end delay, packet delivery ratio, maximum packet sent, maximum packet dropped, and hello load.

5.2.1 Routing Overhead

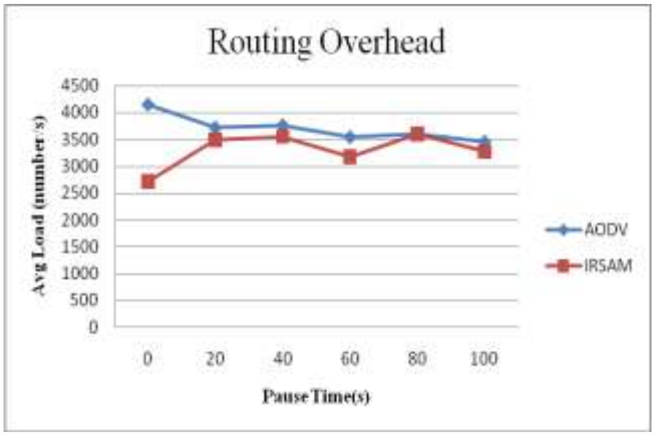


Figure 1: Routing Overhead Senario-1

5.2.2 Average End to End Delay

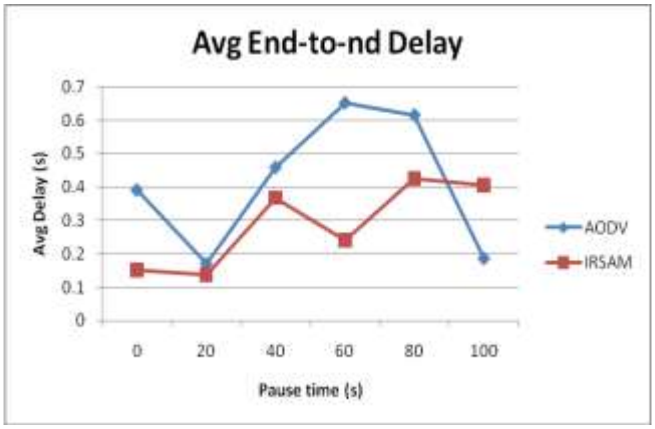


Figure 2: Average End to End Delay Senario-1

5.2.3 Packet Delivery ratio

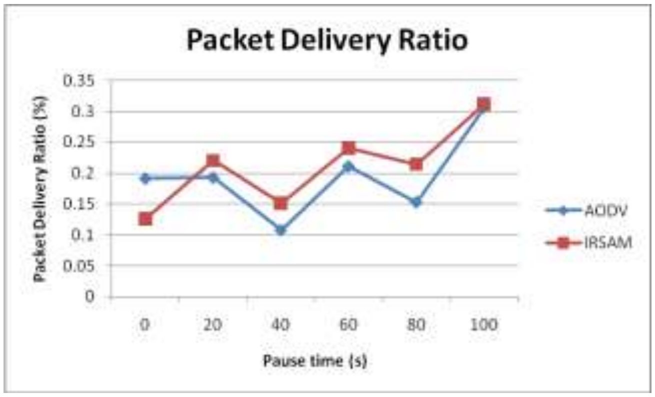


Figure 3: Packet Delivery ratio Senario-1

5.2.4 Maximum Packet sent

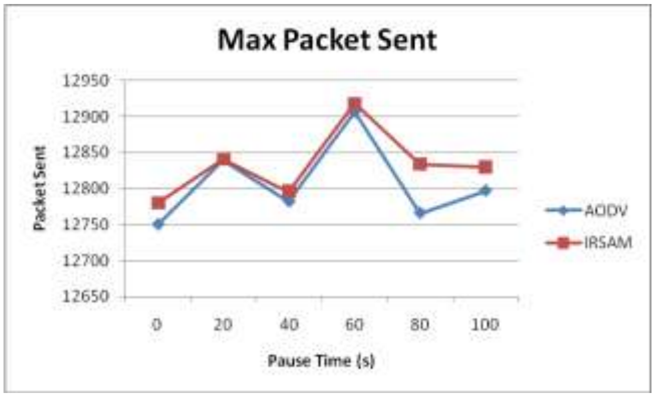


Figure 4: Maximum Packet Sent Senario-1

5.2.5 Maximum Packet Dropped

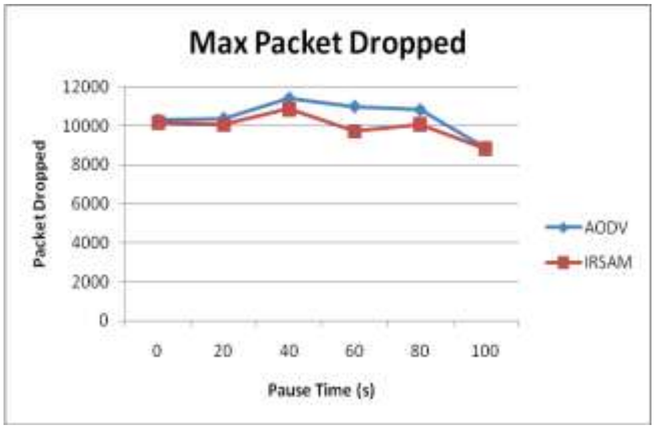


Figure 5: Maximum Packet Dropped Senario-1

5.2.6 Hello Load

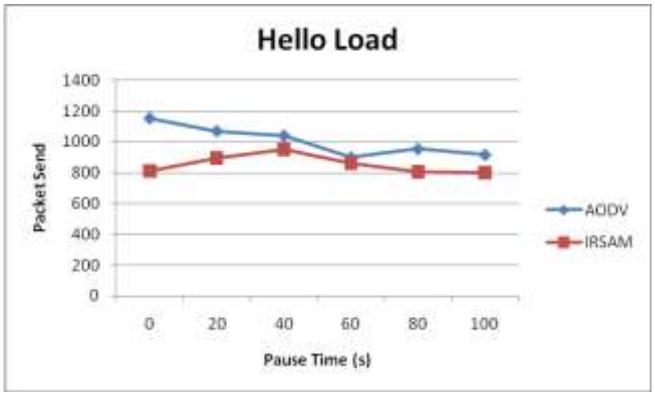


Figure 6: Hello Load Senario-1

5.3 Senario-2: Speed Variation

In Scenario-2 pause time is fixed to 1s but speed is varied from constant 1m/s to 20m/s. This is a very interesting analysis scenario as it shows the performance in terms of nodes mobility. More the mobility, more the link breaks will be and both the protocols can be tested to depth. Again analysis is done using all six parameters End-to-End delay, Packet delivery ratio and Routing overhead, Maximum packet sent, Maximum packet dropped and Hello load.

5.3.1 Routing Overhead

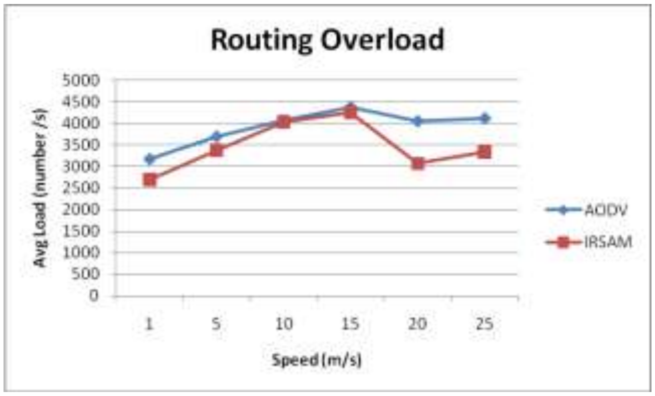


Figure 7: Routing Overhead Senario-2

5.3.2 Average End to End Delay

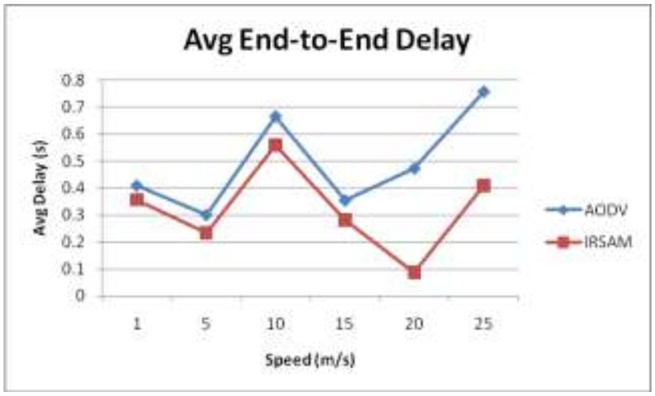


Figure 8: Average End to End Delay Senario-2

5.3.3 Packet Delivery Ratio

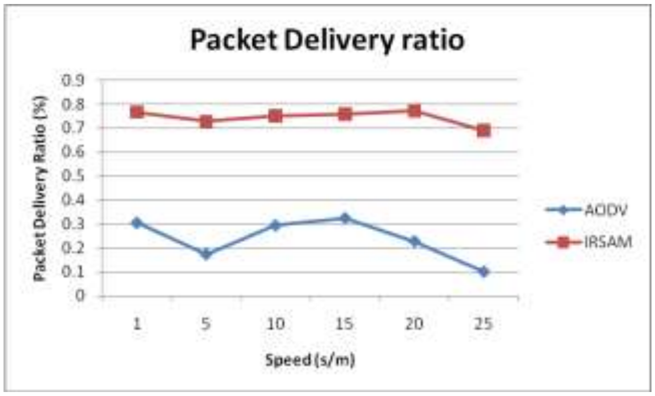


Figure 9: Packet Delivery Ratio Senrio-2

5.3.4 Maximum Packet Sent

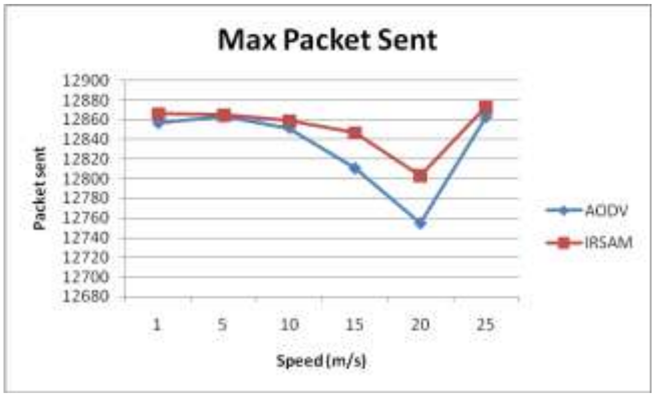


Figure 10: Maximum Packet Sent Senario-2

5.3.5 Maximum Packet Dropped

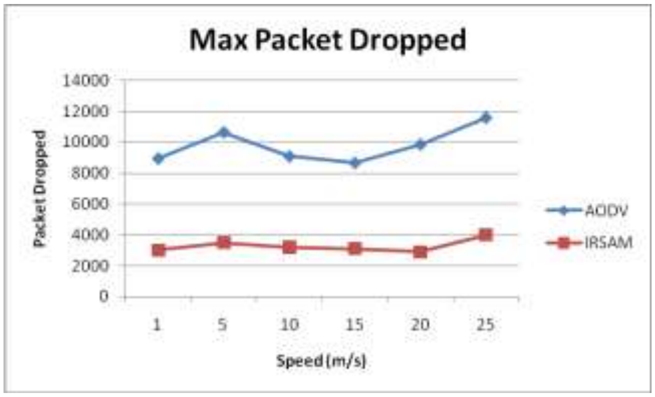


Figure 11: Maximum Packet Dropped Senario-2

5.3.6 Hello Load

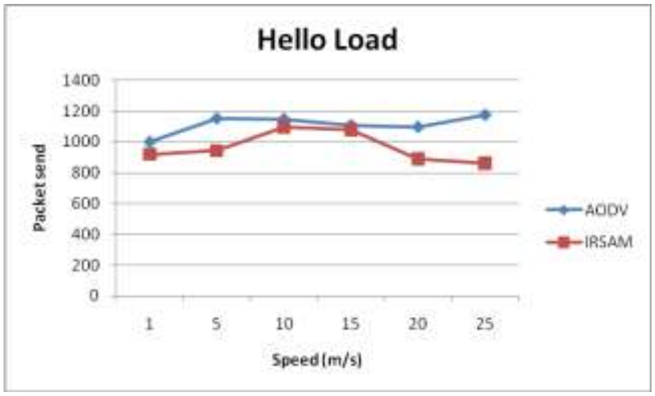


Figure 12: Hello Load Senario-2

6. CONCLUSION

This work proposes an Intrusion response system in AODV for MANET (IRSAM) to enhance the security against the malicious node using NHELLO and Link layer feedback techniques, and utilizing power adaption to keep away the malicious node from transmission range of normal nodes. The Result proves that IRSAM performs better than classic AODV in all of the parameters like routing overhead, end to end delay, packet delivery ratio, maximum packets sent, maximum packets dropped, and hello load. We have less concentrated on IDS, mainly focused on IRS concept, we have utilized an IDS system i.e. used to detect malicious node available in MANET. Our purposed IDS, works for only one type of attack i.e. blackhole. The adaptive power technique used to decrease the transmission range of nodes to keep away the malicious node in MANET without having geographical knowledge. In this work we have created two scenarios; one is the Pause time Variations and the other is Speed Variations. By using six parameters, the results have been evaluated as shown in figure 1 to figure 12. The two scenarios have shown complete comparison study of classical AODV (without IRS) and IRSAM. The evaluation showed that an adaptive power is able to considerably reduce unwanted side-effects of a location-based intrusion response. The geographical based approach suffers from increased loss rates due to the non power-aware AODV routing protocol. We therefore plan to support our approach by power-aware routing protocols. This way, we want to scrutinize the applicability of our approach in real-world scenarios. We further plan to work on a complete IDS system for each kind of attacks and IRS for MANET. Therefore it seems to be a prospective application that can intrinsically handle the challenging conditions in MANETs for envisaged application scenarios like emergency response or defense operations.

7. ACKNOWLEDGEMENTS

Our thanks to the experts those have contributed towards development of the IRSAM. The constant guidance and encouragement received from Mr. Jagpreet Singh, Ph. D. Scholar at IIT Ropar, and Mr. Ashok Kumar, Programmer, at GTBKIET Malout has been an immense help in carrying out the present work and is acknowledged with reverential thanks.

8. REFERENCES

[1] A. Srinivasan, Jie Wu, "A Survey on Secure Localization in Wireless Sensor Networks," in Encyclopedia of Wireless and Mobile Communications, CRC Press, 2007

[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei "A survey of attacks and countermeasures in MANET", Wireless Network Security Signals and Communication Technology, 2007, Part II, 103-135, DOI: 10.1007/978-0-387-33112-6_5

[3] C.E. Perkins, Ad Hoc Networking. Addison Wesley Professional, Dec. 2000. IEEE On page(s): 598 - 610 , Volume: 23 Issue: 3, March 2005

[4] Douglas M.Blough, Mauro Leoncini, Giovanni Resta, Paolo Santi, "The K-Neigh Protocol for Symmetric Topology Control in Ad Hoc Networks," in Proc. of MobiHoc, 2003.

[5] Heady, R., Luger, G., Maccade, A., Servilla, M., "The architecture of a Network Level Intrusion Detection System", Technical report, Computer science Department, University of New Mexico, August 1990

[6] I. A. Getting, "The Global Positioning System," IEEE Spectrum, vol. 30, no. 12, pp. 36–38, 43–47, December 1993

[7] I. Siomina and D. Yuan, "Maximizing Lifetime of Broadcasting in Ad Hoc Networks by Distributed Transmission Power Adjustment," in Proc. of ICTON, 2006

[8] Jagpreet Singh, Paramjeet Singh and Shaveta Rani "Enhanced Local Repair AODV (ELRAODV)" 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies.

[9] Kevin Fall and Kannan Varadhan, "The ns Manual", editors, NS-Documentation, http://www.isi.edu/nsnam/ns/ns-documentation.html.

[10] Martin Mauve and Jorg Widmer, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks," IEEE Network Magazine, vol. 15,no. 6, pp. 30–39, November 2001

[11] Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC3561, IETF MANET Working Group, July 2003.

[12] R. Ramanathan and R.Rosales-Hain, "Topology Control of Multihop Wireless Networks using Transmit Power Adjustment," INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 2000

[13] S. Basagni, I. Chlamtac, V. R. Syrotiuk, B. A. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)," International conference on Mobile Computing and Networking pages: 76-84, 1998.

[14] S-J. Park and R. Sivakumar, "Load-Sensitive Transmission Power Control in Wireless Ad-hoc Networks," in Proc. of GLOBECOM, 2002.

[15] S. Singh, Mike Woo, C.S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," Dallas, Texas, United States Pages: 181 - 190 Year of Publication: 1998 ISBN:1-58113-035-X in Proc. of MobiCom, 1998

[16] Wang, Hong Peng, Cui, Lin., "An enhanced AODV for mobile ad hoc network" international Conference on Machine Learning and Cybernetics, 2008 Volume 2, 12-15 july 2008 Page(s):1135 – 1140.

[17] Young-Bae Ko, Nitin H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," Volume 6, Issue 4 (July 2000) Pages: 307 - 321 Year of Publication: 2000 ISSN: 1022-0038 in Proc. of MobiCom, 1998.

[18] Zhang, Y., Lee, W., "Intrusion Detection on Wireless Ad hoc Networks", in Proceedings 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), August 2000