Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 3, Issue 2, 2017, pp 65-69
ISSN: 2395-0196

Detection and Prevention of Denial of Services Attack based on Signal Strength and Reputation Mechanism

Devendra Poonia
Research Scholar, Department of CSIT, Suresh Gyan Vihar University, Jaipur
deven.poonia99@gmail.com
Manoj Kumar Sharma
Professor, Department of CSIT, Suresh Gyan Vihar University, Jaipur
manoj.sharma@mygyanvihar.com

Abstract: Mobile Ad-Hoc Network is a wireless networking exemplar of mobile hosts which are connected by wireless links without usual routing infrastructure and link fixed routers. Ad-Hoc Distance vector Routing (AODV) is one of the extensively used routing protocol for packet transfer from source to destination. Wireless sensor networks are widely applicable in monitoring and control of environment parameters. In this paper, our main aim is to ensure secure data transmission between the source and destination. There is a need to provide an incentive mechanism which can provide cooperation among the nodes in the network and improve overall network performance by reducing DOS attack. In this Research, we propose a reputation-based incentive mechanism with signal strength mechanism for detecting and preventing DOS attacks. In this paper we propose a new design, implementation, and evaluation of a secure, lightweight, and DOS-resistant security mechanism for various attacks that can be possible on AODV.

Keywords: Security, Mechanism, MANET, Routing Protocols, Ad-Hoc Networks, Mobility, Efficiency.

I. INTRODUCTION

Mobile ad-hoc network is a wireless networking exemplar of mobile hosts which are connected by wireless links without usual routing infrastructure and link fixed routers. Mobile ad-hoc networks are usually collected on a temporary basis to serve a specific deployment purposes like in emergencies such as natural hazards rescue or battlefield communication [1]. It provides a stable communication in situations where the deployments of infrastructure based system is impractical.
Secure routing is vital to the acceptance and use of sensor networks many sensor network routing protocols have been proposed. WSNs use multi-hop routing and wireless communication to transfer data, thus incur more routing attacks.
The paper [3] define the security attributes of routing protocols in WSNs which with them the attackers cannot achieve their goals. Security attributes are the mechanisms that allow the routing protocols to defend against the possible threats in the whole network. These attributes consist of bi-directionality confirmation, base station decentralization identity verification, topology structure restriction and multi-path transmission.
The article [3] proposed security goals for routing in sensor networks and presents the detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks. It also describes practical attacks against all of them that would defeat any reasonable security goals and discuss Counter measures and design considerations for secure routing protocols in sensor networks. There are a lot of approaches to ease routing security [2], [3] and [4].
Undetected node compromise issues: The current cryptography mechanisms, such as authentication, identification, etc. may detect and defend against node compromise in some extent. However, most compromise activities cannot be detected immediately. Designing secure routing that can defend against undetected node compromise is a promising research area.
Most current proposals are suitable for static WSNs. Designing secure routing algorithms for mobile WSNs is

complex and current secure routing algorithms will meet issues when they are applied in mobile environments.

Currently most proposals only consider security metrics and only a few of them evaluate other metrics. Quality of service need to be considered in addition of security.

Routing maintenance: During the lifetime of a sensor network, the network topology changes frequently, and routing error messages are normally produced. Preventing unauthorized nodes from being producing this type of message. This research is to develop of a routing protocol algorithm to solve the problem of secure and efficiency connection establishment in Mobile Ad Hoc networks [5].

As an On-Demand routing protocol establishes routes only when the source node is going to send data packets to a destination node. The goal of these routing protocols is to establish a secure and high quality route in a frequently-changing topology in an Ad Hoc network.

On-Demand routing protocol has less overhead over the Table-Driven routing protocol. The characteristics of network topology change frequently.

II. RELATED WORK

In this research, a modified Ad Hoc On-Demand Distance Vector protocol, called r-aodv, will be developed. R-AODV uses two detection techniques (Reputation Model and Signal Strength) at the same time to detect and prevent DOS attack. We make two contributions. The first is the detection of malicious nodes in the form of attacks on self-created routing infrastructure. The second is to enhance the performance.

In this paper, we propose and implement a new security mechanism in routing protocol algorithm to solve the problem of secure connection establishment in Mobile Ad Hoc networks. As an On-Demand routing protocol establishes routes only when the source node is going to send data packets to a destination node. In this each node acting as a message sender or relay node, each node should change its channel not only depending on the available channel resource, but also on those channels which had been using by its multi-hop neighbors. The neighbor monitoring has also been detected the routing path in the routing protocol for message forwarding to transfer the data packets [8].

A simulation study is utilized to assess the information misfortune, dangers like egotistical and pernicious nodes and information conveyance proportion when utilizing the aodv protocol. The execution of the protocols, previously, then after the fact utilizing identification methods to recognize and evacuate DOS attacks, will be analyzed. The aodv protocol will be altered by including two discovery systems. Moreover, r-aodv specialist is added to the aodv protocol to screen the course and to redesign the right course.

In the traditional AODV protocol, comfort zone of nodes are calculated by Signal strength but no such reputation model was not used with SS on on-demand routing protocol to remove DOS attacks. However, using the R-AODV protocol, always a trusted route will be discovered; focused must be on reliable data transfer, and the data packets will continue to be sent after the corrupt nodes are removed out successfully.

III. PROPOSED METHODOLOGY

Route Discovery is concluded in three steps node information scanning, node Change process and Verification which is achieved by using neighbor monitoring mechanism at middle node.

a). Node information scanning: Suppose the node A is a compromised node. If node A transmits incorrect NIM to neighbors, among its multi-hop neighbors there are some 3NIM-check nodes who is responsible to information scanning, such as nodes C and H. Node C has the largest neighbor numbers and node H has high priority information because it is on the heavily loaded link leading to gateway G. When node C receives the NIM message, it will find out the discrepancy in the information assigned to interface RA-3. The anomaly can be detected because the current information being used on RA-3 is C3, not C1.Similarly, node H will find the discrepancy in the information assigned to interface RA-1.After the NIM check, those performers can execute the normal communication procedure and maintaining the security value of the nodes being checked.

b). Node Change process: Security-value also indicates the trustable degree of a particular node, where 0 security-value ≥ K. Value 0means the NIM message of a particular node is correct and this node is security and well behaving. Value K means this node is compromised and trustless, while the intermediate value mark this node as suspicious. No node would be titled as "compromised node" before its security-value is incremented to K. Like bad-credit, the selection of K is also left as a design parameter.

c). Verification: If the discrepancy of a NIM has been checked out, a security alarm message (SM), which contains the identity of discrepancy information and the identity of suspicious node, would be created by NIM-check nodes. The next task of those NIM-check nodes is to broadcast the latest SM to their neighbors. Each node also maintains the security-value of nodes within its interference domain neighbors.

It ensures that any malicious node is not present in the network. When the verification process succeeds, destination node send RREP message to the source node through the same discovered route. RREP message is forwarded in the network until source node is not encountered.

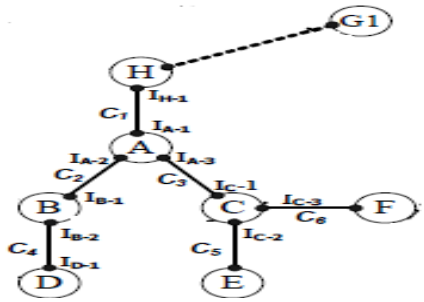


Fig. 1: Route Discovery in neighbor monitoring mechanism AODV Protocol

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 3, Issue 2, 2017, pp 65-69
ISSN: 2395-0196

R-AODV mechanism is stepwise explained as follows:
A source ready for data transmission generates a data packet Node Information Message NIM message to its intermediate neighbor nodes node to disseminate its information assignment information. Intermediate neighbor nodes after receiving NIM message checks if route exists or not. It creates a fresh route if not present by initializing Route Discovery Process. In route discovery process first of all The neighbor nodes of a certain node can perform node information scanning to check whether there exists abnormal of information assignment of that node in NIM. In Figure 2, Intermediate nodes for node S are {B, H, E and C}.
In node information scanning, the neighbor nodes can switch information sequentially on their radio and intercept at an information for a short duration of time to check the misbehavior of NIM. It is obviously that performing information scanning for every node on certain of receiver nodes is not enough. In this section, we propose a new mechanism for NIM check. At first, we enlarge the scope area and participants of the check. According to the interference model (Fig. 1), both one-hop neighbors and two-hop neighbors can perform information scanning, such as one-hop neighbors {B,C,H} and two-hop neighbors{S,E,F} in Fig. 1
In order to enhance the reliability and efficiency, our new mechanism set a rule to choose some nodes acting as the NIM check performers. It includes:
a) Those nodes with the heavily loaded high priority information or links.
b) Those nodes with the biggest neighbor numbers, under normal operation, a node assigns the least loaded information to its interfaces and transmits the latest CM information to its neighbors. Those neighbor nodes can check the correctness of the related information in CM [11-23].

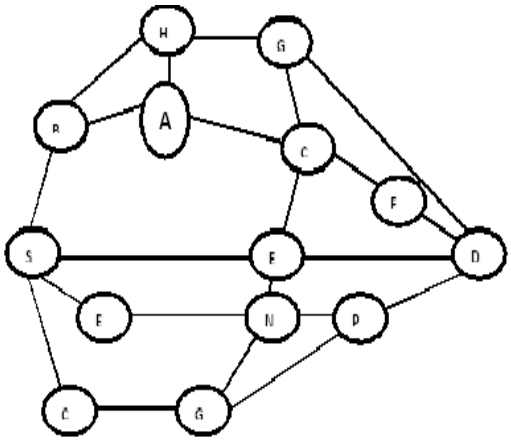


Fig. 2: Design of the Multi Nodes Monitoring

1. A loop is initialized until destination node is not obtained.
2. It ensures that any malicious node is not present in the network. When the verification process succeeds, destination node send RREP message to the source node through the same discovered route. RREP message is forwarded in the network until source node is not encountered.

IV. **RESULTS**

We have analyzed our proposed work with the help of Exata simulator that generate simulation results of network called r-aodv. The results are generated on large number of scenarios with various parameter values to show its effectiveness in all kinds of situations.

a) Simulation Parameters

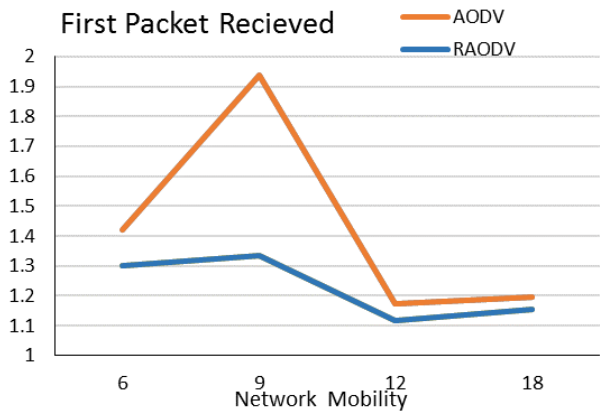
SIMULATION PARAMETERS	
Examined protocols	AODV and R-AODV
Number of Nodes	50
Traffic Type	TCP
Performance Parameter	Throughput, EED, Network Load
Pause time	30 seconds
Mobility (m/s)	10 meter/second
Date Rate (Mbps)	6-24 Mbps
Packet size (bits)	1024
Simulator	EXATA
Simulation area (m x m)	1200 x 1200
Maximum Packet Value	50
Mobility Model	Random waypoint

Table 1: Simulation Parameters

b) Simulation Results

Network Mobility Scenario One (AODV AND R-AODV):
Using the exata simulator, a MANET with random waypoint model is designed for 50 nodes. Within an area 1200mX1200 m. The performances of AODV and R-AODV is evaluated

with network mobility with respect to End to End Delay,



Throughput and FPR at pause time equals 30.

Fig. 3 First Packet Received of R-aodv and Aodv with attack for 50 node.

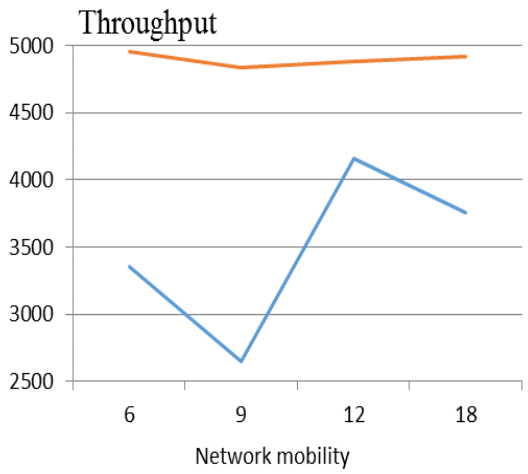


Fig. 4 Throughput of r-aodv and aodv with attack at 50 nodes.

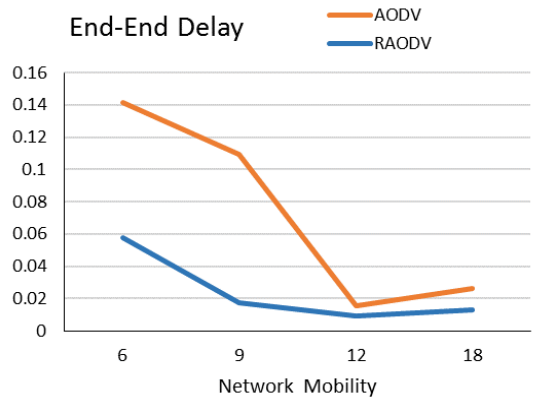


Fig.5 End-to-end delay of R-AODV and AODV for 50 nodes.

Network Load Scenario Two (AODV AND R-AODV):

Using the exata simulator, a MANET with random waypoint model designed for 50 nodes within an area of 1200mX1200 m. The performance of both AODV and R-AODV protocols is evaluated with network load with respect to End to End Delay, Throughput and FPR. Pause time equals 30.

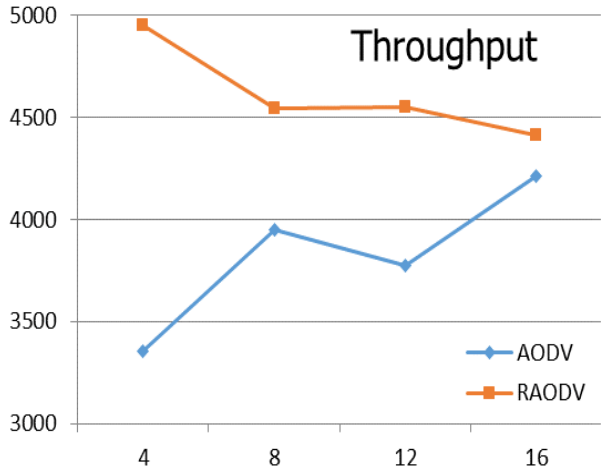


Fig. 6 Throughput of R-aodv and Aodv with network load in 30s pause time.

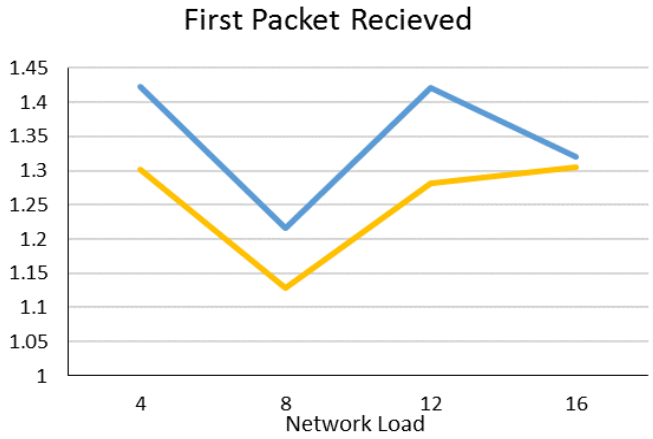


Fig. 7 First packet received in 30 s Pause Time

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

Security of MANET is one of the imperative one component for its organization. In our theory, we have analyzed both the direct and troubles of security threats in versatile Ad-Hoc

coordinates with best proposed course of action finding framework. This theory work gives the report along results accomplished from the exploration directed on the aodv protocol in specially appointed system. Some investigation and correlations of execution of AODV and R-AODV directing protocols in MANETs have been done in this examination, that are likely in light of the execution measurements as opposed to any security metric. R-AODV executes all things considered like AODV when there is low number of nodes and less versatility however then moving to higher number of nodes and increment in portability, it slopes to separate.

This theory work gives the report along results accomplished from the exploration directed on the aodv protocol in specially appointed system. Since, utilizing the aodv protocol in an Ad Hoc organize, the execution is completely influenced due to degree of the change to network topology. Hence, the execution of AODV can be upgraded by utilizing adjusted aodv, which utilizes flag power and notoriety based plan.

B. Future Scope

In this research, we introduced another strategy to enhance execution of the aodv protocol by utilizing signal quality and notoriety based component in Ad Hoc arrange. This strategy can be utilized as a part of some other remote systems to enhance their execution. We attempted to find and examine the effect of dos attack in manets utilizing both aodv and r-aodv protocols. There is a need to break down dos attack in other manet routing protocols simply like dsr, tora and grp. Different sorts of attacks, for example, wormhole, jellyfish and sybil attacks ought to be considered in examination with DOS attack. They can be sorted on the premise of the amount they can influence the execution of entire system.

DOS attack can likewise attack the other route around i.e. lack of sleep attack. The identification of this conduct of DOS attack and also the end techniques for such conduct must be completed for further research. The aodv protocol was decided for work due to its straightforwardness and it is additionally a draft directing protocol in RFC (Request for Comments). It gives numerous routing protocols to both wired and remote systems particularly for Ad Hoc arrange.

Really in a genuine Ad Hoc arrange environment portable nodes are restricted by power supply, memory space, CPU execution, data transfer capacity and so forth. In this exploration work, tests were completed to decide the impacts of the unforeseen broken courses and furthermore to reroute information packets to Ad Hoc organize. In the research, the emphasis is on solid information security and secure transmission way.

REFERENCES

[1] Kar, K., Luo, X., Sarkar, S, "Throughput-Optimal Scheduling in Multichannel Access Point Networks Under Infrequent Channel Measurements", INFOCOM 2007, 26th IEEE International Conference on Computer Communications, May 2007, pp. 1640 –1648.

[2] Lin, X., Rasool, S.A, "Distributed Joint Channel-Assignment, Scheduling and Routing Algorithm for Multi-Channel Ad-hoc Wireless Networks". INFOCOM 2007, 26th IEEE International Conference on Computer Communications, May 2007, pp. 1118 –1126.

[3] P. Dutta, S. Jaiswal, R. Rastogi, "Globally Optimal Channel Assignment for Non-Cooperative Wireless Networks", INFOCOM 2008, pp. 2216-2224.

[4] T. Jin, G. Noubir, B. Thapa, "Zero Pre-shared Secret Key Establishment in the Presence of Jammers", MOBIHOC 2009, New Orleans, Louisiana, USA, 2009, pp. 219-228.

[5] A. Dhananjay, H. Zhang, "Practical, Distributed Channel Assignment and Routing in Dual-radio Mesh Networks", SIGCOMM 2009, Aug 2009, pp. 99 – 110.

[6] H. Huang, X. Cao, and X. Jia,"Channel assignment using block design in wireless mesh networks", Computer Communication, vol.32, 2009, pp.1148-1153.

[7] M. Alicherry, R. Bhatia, L. Li,"Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks", MOBICOM 2005, Cologne, Germany, Aug 2005, pp. 58-72.

[8] YingZhi Zeng, JinShu Su, Xia Yan, BaoKang Zhao, QingYuan Huang. "LBKERS: A New Efficient Key Management Scheme for Wireless Sensor Networks". the 3rd International Conference on Mobile Ad-hoc and Sensor Networks (MSN), Beijing, China, 2007, pp. 772-783.

[9] A. Naveed, S. S. Kanhere, "Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks", Globecom 2006, Nov. 2006, pp..

[10] A. Haq, A. Naveed and S. S. Kanhere, "Securing Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks", in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2007), Hong Kong, March 2007, pp. 3113-3118.

[11] MK Sharma, Adaptive Steganographic Algorithm using Cryptographic Encryption RSA Algorithms Journal of Engineering, Computers & Applied Sciences (JEC& AS) 2 (1), 1-3, 2013.

[12] MK Sharma, Classification of image using a genetic general neural decision tree, Int. J. Applied Pattern Recognition 2 (1), 76, 2015.

[13] MK Sharma, An efficient segmentation technique for Devanagari offline handwritten scripts using the Feedforward Neural Network, Neural Computing and Applications 26 (2), 1-13, 2015.

[14] MK Sharma, Pixel plot and trace based segmentation method for bilingual handwritten scripts using feedforward neural network, Neural Computing and Applications 27 (7), 1817-1829, 2016.
[15] MK Sharma, Advanced Neuro-Fuzzy Approach for Social Media Mining Methods using Cloud, International Journal of Computer Applications (0975–8887) Volume 2, 2016.
[16] MK Sharma, Segmentation of english Offline handwritten cursive scripts using a feedforward neural network, Neural Computing and Applications, 1-11, 2015.
[17] MK Sharma, Offline scripting-free author identification based on speeded-up robust features, International Journal on Document Analysis and Recognition (IJDAR), Volume 18, Issue 4, pp 303–316, 2015.
[18] MK Sharma, Offline Language-free Writer Identification Based on Speeded-up Robust Features International Journal of Engineering (IJE), IJE TRANSACTIONS A: Basics 28 (7), 2015.
[19] M Sharma, Character Recognition of Offline Handwritten English Scripts: A Review, International Journal of Advanced Networking and Applications (IJANA), 94-103, 2014.
[20] MK Sharma, A Survey of Thresholding Techniques over Images, INROADS 2 (2), 461-478, 2014.
[21] M Sharma, Offline Handwritten English Script Recognition: A Survey, International Journal of Advanced Networking and Applications (IJANA), 114-124, 2014.
[22] M Sharma, A Framework for Big Data Analytics as a Scalable Systems, International Journal of Advanced Networking and Applications (IJANA), 72-82, 2014.
[23] M Sharma, Speech Recognition: A Review, International Journal of Advanced Networking and Applications (IJANA), 62-71, 2014.
[24] Rakhi Purohit, Bright Keswani, “Analysis of Impact of Varying CBR Traffic with OLSR & ZRP”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 3 (March 2016) pp. 82-85.
[25]. Rakhi Purohit, Bright Keswani, “Impact of Node Mobility with OLSR Protocol”, International Journal of Computer Applications (0975 – 8887) Volume 128, No.11 (October 2015) pp. 14-17.
[26]. Rakhi Purohit, Bright Keswani, “Node Mobility Impact on Zone Routing Protocol“, International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 18 (May 2015) pp. 29- 32.