ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Link Correlation Aware Opportunistic Routing in Wireless Network

Supragya Verma[1], Prof. Jai Mungi[2]

M. Tech. Scholar, Department of Computer Science and Engineering, SIRTE, Bhopal India[1]

Assistant Professor, Department of Computer Science and Engineering, SIRTE, Bhopal India[2]

ABSTRACT: Ad hoc On-Demand Distance Vector, AODV, is a distance vector routing protocol that is reactive. AODV requires each node to maintain a routing table containing one route entry for each destination that the node is communicating with. In this paper we proposed the enhanced of AODV routing protocol using multiple constraints function. The multiple constraints function measures the minimum distance between neighbor nodes and control the function of mobility.

KEYWORDS:- MANET'S, DDOS, Routing Protocol, AODV.

I. INTRODUCTION

Security and privacy are complex issues in ad hoc wireless networks. This complexity is the result of a number of factors, including the wireless medium, nodes mobility and lack of infrastructure. A malicious node (or attacker) can easily eavesdrop into the wireless communication channels and infer communication. Additionally, because of the mobility of the nodes and the absence of infrastructure, communicating nodes rely on other mobile intermediate nodes to relay their data. This openness in ad hoc wireless networks makes the nodes more susceptible to attacks by hackers. There are different kinds of attacks that can be used by malicious nodes (or users) to harm the network, and leave its ad hoc routing protocols unreliable. They can be basically categorized, based upon the nature of the attacks, into passive attacks and active attacks [1]. Due to the nature of the wireless environment and the lack of predefined infrastructure [12,13], achieving secure routing in wireless ad hoc networks is a complex task A number of protocols have been developed to add security to routing in ad hoc networks. Papadimitriou and Haas [14] proposed SRP (Secure Routing Protocol) based on DSR [15, 16]. The protocol assumes the existence of a security association between the source and destination to validate the integrity of a discovered route. Mobile ad hoc networks (MANETs) are finding ever-increasing applications in both military and civilian systems due to their self-configuration and self-maintenance capabilities. Many of these applications are security sensitive, such as military battlefield operations, homeland security scenarios, law enforcement, and rescue missions. The shared wireless medium of MANETs introduces opportunities for passive eavesdropping on data communications. Adversaries can easily overhear all the messages "flying in the air" without physically compromising a node. Several methods have been investigated to withstand eavesdropping and further the traffic analysis. One attempt is to prevent the wireless signals from being intercepted or even detected by developing some LPI/LPD (low probability of interception/low probability of detection) communication techniques. Examples of such techniques include the spread-spectrum modulation, effective power control, and directional antennas [4]. However, it is impossible to completely avoid signal detection in the open wireless environments. The second one relies on the use of traffic padding, i.e., introducing dummy packets into the network [5] to camouflage the real traffic pattern. However, this approach adds significant extra load to the network and consumes the scarce network resources. A third method is to perform end-to-end encryption and/or link encryption on data traffic. However, it only prevents adversaries from accessing Traffic contents.

The rest of this paper is organized as follows in section II we discuss about the rich literature survey for the existing Routing protocol. In section III we discuss about the about problem statement. In section IV we Discuss about the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

proposed methods, In section V we show the result analysis and finally in section VI conclude the our research work and also define the future scope of this work.

II. RELATED WORK

[1] In this paper author presents a new detection method based on Kernel Principle Component Analysis (KPCA) and Particle Swarm Optimization (PSO)-Support Vector Machine (SVM). The KPCA was used to obtain the important characteristics of the intrusion data to eliminate the redundant features. Then the PSO was used to optimize the SVM parameters. Experimental results show the proposed approach can enhance the detection rate, and performs better than the PCA based methods.

[2] In this paper, a cross layer protocol is designed to detect denial of service attack imposed on the network by malicious nodes. The Denial of Service attack on sensor networks not only diminishes the network performance but also affects the reliability of the information. Swarm intelligence, an evolutionary algorithm is used in predicting the traffic patterns and detecting malicious nodes. This novel approach helps in keeping the network functional and self-sustaining by re-routing the information.

[3] In this paper, a new network intrusion system based on ABC searching algorithm has been proposed and implemented. The performance of the proposed Anomaly-based NIDS (A-NIDS) using ABC algorithm (called A-NIDS-ABC for short) has been tested using KDD-99 datasets developed by MIT Lincoln Labs. They have also compared the proposed A-NIDS-ABC with other five traditional classification algorithms. The experimental results showed that the proposed method can outperform other five popular benchmark classifiers and is suitable for the network intrusion detection.

[4] This paper proposes a suite of algorithms which optimize the performance of dynamic content applications by considering both server CPU loads and network latencies. The goal of the algorithms is to reduce client access times while also minimizing the resource utilization. The algorithms are designed for a hosting architecture comprising a grid of clusters interconnected via high bandwidth links and each cluster hosting a complete application replica.

[5] In this paper, they present a literature on classification of available mechanisms for DDoS defense. These defense mechanisms are used to prevent, detect, response and tolerate the DDoS attacks. It is well known that it is very difficult to stop the DDoS attack; therefore, it would be better to maximize the fault tolerance and quality of services under variety of intrusions and attacks. In Their analysis, They will discuss the merits and demerits of each mechanism over others.

[7] In this paper, they provide a security scheme against DoS attacks (SSAD) in cluster-based WSNs. The scheme establishes trust management with energy character, which leads nodes to elect trusted cluster heads. Furthermore, a new type of vice cluster head node is proposed to detect betrayed cluster heads. Theoretical analyses and simulation results show that SSAD can prevent and detect malicious nodes with high probability of success.

[8] In this paper, they suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation, they demonstrate that 1) the proposed protection prevents more than 95 percent of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable. Last, They suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

III. PROBLEM STETEMENT

The aim of this dissertation is to propose an effective and efficient scheme which Provide secured privacy of node location .The location privacy of end nodes remains to be solved even when identification anonymity issues are addressed in the wireless routing protocol. Location privacy attacks can be performed by tracing either route discovery messages or data packets in order to discover the message's Origin or destination venue.

- Hiding the entity of interest among a number of similar entities
- The anonymity set, so that it is not obvious to outsiders which anonymity set member is the real entity.
- The routing in a way that the location of the destination node cannot be discovered by the adversary.
- This protocol supports receiver location privacy even against a global traffic analyzer.

IV. PROPOSED METHODS

In this dissertation we proposed the enhanced of AODV routing protocol using multiple constraints function. The multiple constraints function measures the minimum distance between neighbor nodes and control the function of mobility. We have estimated the median contention count using the maximum and minimum number of neighbors (the respective requesting nodes possess) in their transmission range. Each additional retransmission consumes additional bandwidth and energy and increases transmission latency and error rates. To avoid the unnecessary consumption of bandwidth and energy, we have also tried to minimize the length of the route along with the discovery of a reliable route.
The multiple constraints function used some derivate for the estimation of function cost for route discovery, path establishment and finally path maintained. Initially used the distribution function for the deployment of node in wireless area network.

Steps 1 Distribution of data sample
Let us consider $\{x^*(i,j) \mathrm{I}\ i = 1, 2, \ldots\ldots, n\ ; j = 1, 2, \ldots, p\}$ is sample set of node for the distribution in given area used mapping function using equation (1) and (2)
For the estimation of hop used these formulae

$$x(i,j) = \frac{(x^*(i,j) - x_{min}(j))}{(x_{max}(j) - x_{min}(j))} \quad (1)$$

For the validation of the total hop used for the communication:

$$x(i,j) = \frac{((x_{max}(j) - x^*(i,j))}{(x_{max}(j) - x_{min}(j))} \quad (2)$$

Where $x_{min}(j)$ the minimum value of is node j, and $x_{max}(j)$ is the maximum value of node j.

Step 2 estimates the value of route cost $R(a)$.
$\{x(i,j) \mathrm{I}\ j = 1, 2 \ldots, p\}$ is distributed into route path get hope values $z(i)$ through distribuation $a = [a(1), a(2), \ldots\ldots, a(p)]$ as:

$$z(i) = \sum_{j=1}^{p} a(j)x(i,j), \quad i = 1, 2, \ldots\ldots n \quad (3)$$

The evaluation final path for the communication is determined by $R(a)$, shown as:

$$F(a) = S_z D_z \quad (4)$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Where S_z is the standard deviation of $z(i)$; D_z is the threshold value; standard deviation S_z and local density D_z are defined in formula (5):

$$\begin{cases} S_z = \sqrt{\frac{\sum_{i=1}^{n}(z(i) - E(z))^2}{(n-1)}} \\ D_z = \sum_{i=1}^{n}\sum_{j=1}^{n}(R - r(i,j))\, u(R - r(i,j)) \end{cases} \quad (5)$$

.

(1) Defining $d(z(k), z(h))$ as the absolute distance between the two mobile node

$$d(z(k), z(h)) = \sqrt{(z(k) - z(h))(z(k) - z(h))} = \sqrt{(z(k) - z(h))^2} \quad (6)$$

$$k = 1, 2, \ldots\ldots\ldots, N; h = 1, 2, \ldots\ldots\ldots, N$$

$N(n \geq N \geq 2)$ is evaluation level number or same mobility area? And $D_q(q = 1, 2, \ldots\ldots, N)$ is used to describe the different group on the basis of hop count $G_q(q = 1, 2, \ldots\ldots, N)$,

Step 4 Determining constraint established the communication in AODV, which gave the constraint conditions s.t. $\sum_{j=1}^{p} a^2(j) = 1$. but it did not specify a value range.

$$\begin{cases} s.t. \sum_{j=1}^{p} a^2(j) = 1 \\ 1 \geq a(j) \geq 0 \end{cases} \quad (7)$$

Step 5 established the communication.

V. RESULT ANALYSIS

To investigate the effectiveness of the proposed scheme for improvement of performance of MANET network using LCAORP routing protocol on a simplified topology was carried out using Network Simulator version NS-2.34.

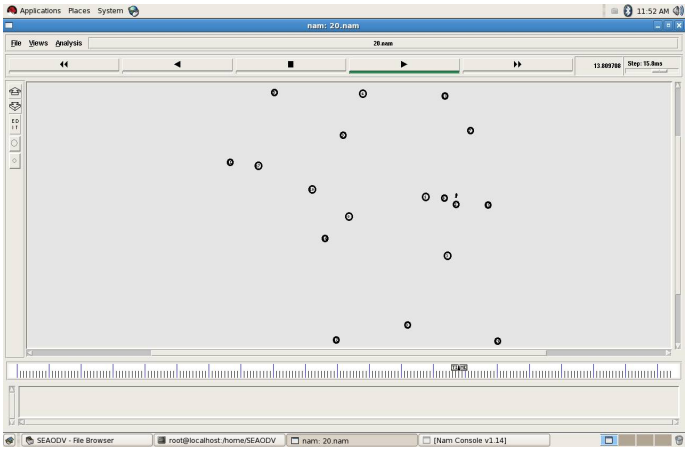

Figure 1: In this figure we shows that the simulation scenario of AODV scheme for pause time 10s.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

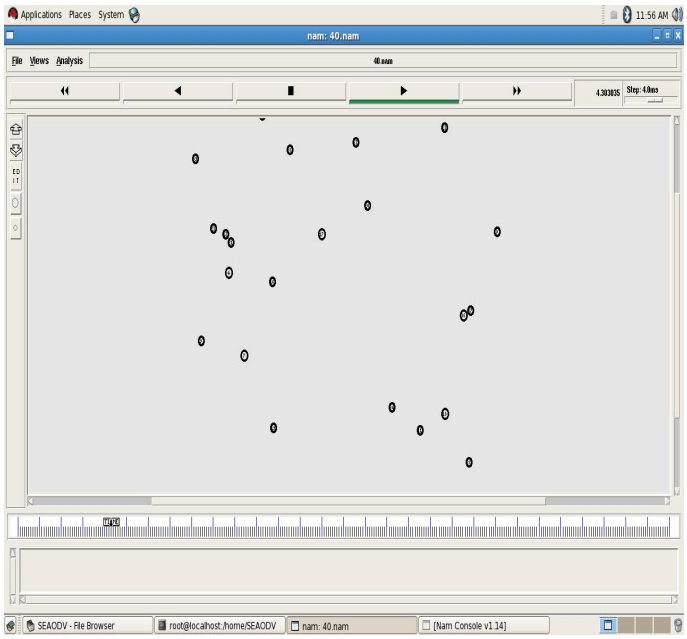

Figure 2: In this figure we shows that the simulation scenario of AODV-MANET scheme on pause time for 20s.

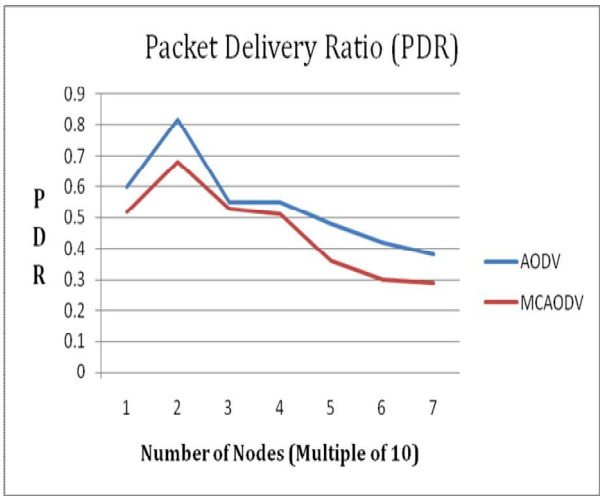

Figure 3: Packet Delivery Ratio vs. Number of nodes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

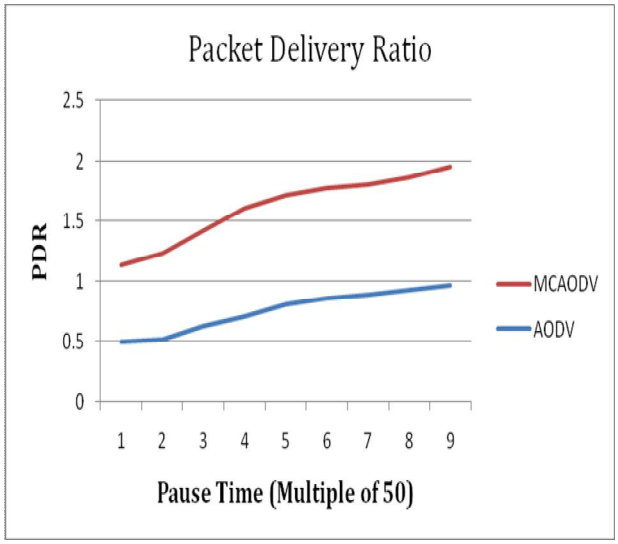

Figure 4: Packet Delivery Ratio vs. Number of nodes.

VI. CONCLUSION AND FUTURE WORK

In this dissertation we proposed the modified the AODV routing protocol for the enhancement of routing protocol in multi-hope communication mode. The threshold based function measure the distance of mobility of node during the process of communication. The mobility of node measure in two different scenarios. In 1st scenario measure the same level of path and 2nd level used in case of different path. For the evaluation of performance our modified protocol tested in different network scenario tested through simulations for different distributions of nodes in different connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent routing probabilities reduced number of transmissions. This work has focused on enhanced the Link Aware OR protocol in mobility condition. Future work includes developing a technique for real time network such as VANET and some other network. In this work it seems to be that network packet has increased. Due to number of packets the performance of network can reduces. It also increases the network conjunction. So there is need to reduce the packets in the network.

REFERENCES

[1] Xiang Xu, Ding Wei, Yuelei Zhang "Improved Detection Approach for Distributed Denial of Service Attack Based on SVM" IEEE, 2011. Pp 1-3.
[2] Rajani Muraleedharan and Dr. Lisa Ann Osadciw "Cross Layer Security Protocol Using Swarm Intelligence" 2007. Pp 1-6.
[3] Changseok Bae, Wei-Chang Yeh, Mohd Afizi, Mohd Shukran, Yuk Ying Chung and Tsung-Jung Hsieh "A NOVEL ANOMALY-NETWORK INTRUSION DETECTION SYSTEM USING ABC ALGORITHMS" International Journal of Innovative Computing, Information and Control Volume 8, Number 12, December 2012. Pp 8231–8248.
[4] Supranamaya Ranjan, Edward Knightly "High Performance Resource Allocation and Request Redirection Algorithms for Web Clusters" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2010. Pp 1-14.
[5] Anupama Mishra, B. B. Gupta, R. C. Joshi "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques" IEEE, European Intelligence and Security Informatics Conference, 2011. Pp 286-289.
[6] Naveen Mohan Prajapati, Atish Mishra, Praveen Bhanodia "A Heuristic Approach for Efficient Detection of Intrusion" International Journal of Computer Applications , Volume 94 – No 3, May 2014. Pp 6-10.
[7] Guangjie Han, Wen Shen, Trung Q. Duong, Mohsen Guizani, Takahiro Hara "A proposed security scheme against Denial of Service attacks in cluster-based wireless sensor networks" SECURITY AND COMMUNICATION NETWORKS, 2014. Pp 2542–2554.
[8] Gaurav Singal, Vijay Laxmi, M.S. Gaur, Swati Todi, Vijay Rao and AkkaZemmari "MCLSPM: Multi-constraints Link Stable Multicast Routing Protocol in Adhoc Networks", Wireless Days, 2016, Pp 1-6.
[9] Abdul HadiAbd Rahman and Zuriati Ahmad Zukarnain "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks", European Journal of Scientific Research, 2009, Pp 566-576.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

[10] Javad Akbari Torkestani and Mohammad Reza Meybodi "Mobility-based multicast routing algorithm for wireless mobile Ad-hoc networks: A learning automata approach", Computer Communications, 2010, Pp 1-15.
[11] James Bernsen and D. Manivannan "Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification", Pervasive and Mobile Computing, 2009, Pp 1-18.
[12] Yun-Wei Lin, Yuh-Shyan Chen and Sing-Ling Lee "Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives", JOURNAL OF INFORMATION SCIENCE AND ENGINEERING, 2010, Pp 913-932.
[13] Wai Chen, Ratul K. Guha, TaekJin Kwon, John Lee and Irene Y. Hsu "A Survey and Challenges in Routing and Data Dissemination in Vehicular Ad-hoc Networks", IEEE, 2008, Pp 328-333.
[14] S. A. Ade and P.A.Tijare "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks", International Journal of Information Technology and Knowledge Management, 2010, Pp 545-548.
[15] E. A .Mary Anita and V. Vasudevan "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining", International Journal of Computer Applications, 2010, Pp 22-29.
[16] MarwaAltayeb and ImadMahgoub "A Survey of Vehicular Ad hoc Networks Routing Protocols", Innovative Space of Scientific Research Journals, 2013, Pp 829-846.
[17] Alex Hinds, Michael Ngulube, Shaoying Zhu and Hussain Al-Aqrabi "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET) ", International Journal of Information and Education Technology, 2013, Pp 1-5.
[18] Ozan K. Tonguz and NawapornWisitpongphan "DV-CAST: A DISTRIBUTED VEHICULAR BROADCAST PROTOCOL FOR VEHICULAR AD HOC NETWORKS", IEEE, 2010, Pp 47-57.
[19] V. Kanakaris, D. Ndzi and D. Azzi "Ad-hoc Networks Energy Consumption: A review of the Ad-Hoc Routing Protocols", Journal of Engineering Science and Technology , 2010, Pp 162-167.
[20] Amit N. Thakare and Mrs. M. Y. Joshi "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks", IJCA, 2010, Pp 211-218.
[21] Busola S. Olagbegi and Natarajan Meghanathan "A REVIEW OF THE ENERGY EFFICIENT AND SECURE MULTICAST ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS", International journal on applications of graph theory in wireless ad hoc networks and sensor networks, 2010, Pp 1-15.