Robust Approach to Secure Routing Protocol in Mobile Adhoc Network using Network Simulator 2 : A Review

Deepak Dalal[1], Dr. Sandeep Tayal[2], Dr. Pawan Kumar[3]
Student[1] – Vaish College of Engineering, Department ECE, Rohtak, Haryana, India
Associate Professor[2]– Vaish College of Engineering, Department ECE, Rohtak, Haryana, India
Assistant Professor[3]– Vaish College of Engineering, Department ECE, Rohtak, Haryana, India

Abstract – Security is one of immense challenges in deploying adhoc network (VANET and MANET) due to vigorous topology and there are other reasons also exist. Due to dynamic topology possibility of attacks increased and various types of attack exist in which unauthorized person can deploy malicious nodes in network. Through active and passive attack in network information can be accessed. There are diverse numbers of active and passive attacks which are very harmful for effective communication between transmitters to receiver. Out of these attacks black hole attack in Vehicular Ad Hoc Network is crucial problem related with the field of computer networking. In reference work protocol was used along with black hole attack for effective network communication. In this article after going through numerous research papers in different domain our main focus would be to developed advance protocol which can with stand against black hole attacks. Today security is one of the prime concern therefore to keep in mind security concern need to developed protocol with security feature so that unauthorized person cannot access data.

Index Terms – Black Hole Attack, Network, Secure, Adhoc, Protocol, VANET, Packet

1. INTRODUCTION

Wireless Ad hoc Network gives a tender which provide cost constructive communication between users. It is distinguished by redistributed architecture, mobile nodes, zestful topology, etc. which makes network formation typically tedious. In the past decade, there has been tremendous research work carried out by researchers towards increasing its routing implementation by solving diverse important problems. WSN is considered as an unfold innovation that have been significantly implemented in tough circumstances for example battlefields and smart homes, traffic surveillance, monitoring, building habitat and many more domains.

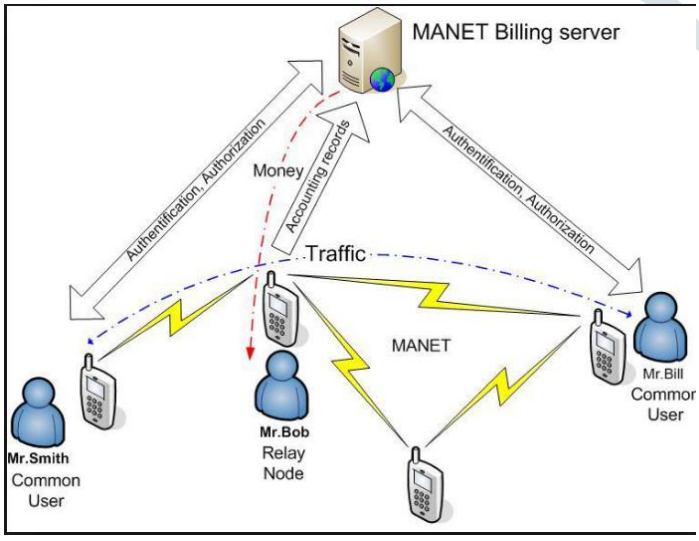

Figure 1 MANET Network Functioning

Wireless system network subsist many sensor nodes. These SNs are sensitive to phenomenal changes causing information transportation to BS that is far away generally. The energy usage is crucial factor in sensor nodes, because these are chargeable through batteries with finite powers. Clustering technique is required along with data accumulation so that the energy consumed is lesser. In our method, SNs can split into clusters. Every cluster has a depictive node called CHs. Its function is to collect information in cluster then transmit this information to base station. Now only cluster head requires large length transportation using multihop causing energy consumption to become less. This also helps in power management. Sensor devices are used to measure physical parameters like pressure, temperature, humidity etc. When placed within the transmission range of each other, it forms a sensor network. It carries the task of sensing, computation and forwarding.

They have some limitations like computation, memory and energy. Sensors deployed in applications like the agricultural field require that the batteries be operating for one cropping season. Energy in the reduction of the packet size, or distance between the nodes can also help in saving sufficient amount of energy. Efficient routing algorithms will have to be incorporated to find paths which consume minimal energy during path establishment and data transfer [1, 2].

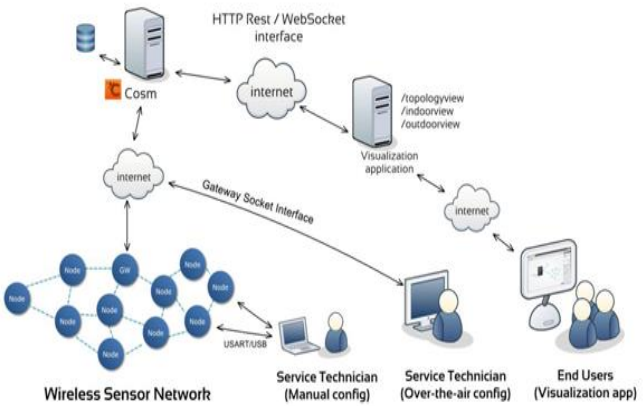

Fig.1.3 Architecture of Wireless Sensor Network

2. ROUTING PROTOCOL IN WSN

There are huge numbers of routing protocols which are used for wireless adhoc network. Wireless sensor routing protocol classified into four domains

- Routing Process
- Network Structure
- Network Operation
- Initiator of Communication

Out of these domains further routing protocol based on routing processing classified into three segments

- Proactive Protocols
- Reactive Protocols
- Hybrid Protocols

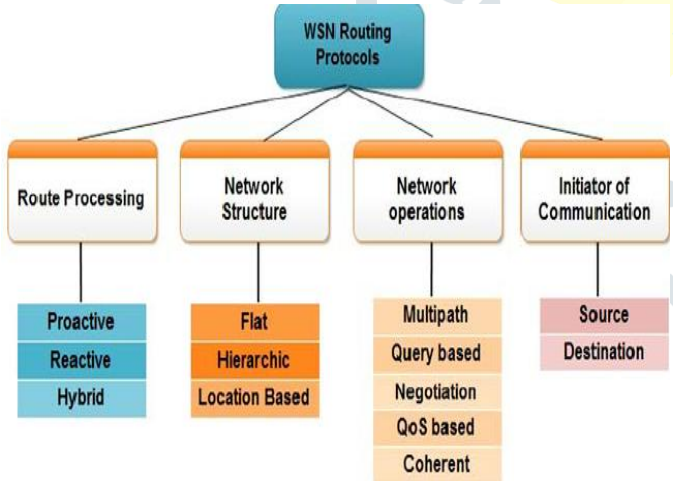

Figure 2 Classification of Routing Protocol

Adequate innovation has already been executed by researchers which compromise relative differentiation of different routing protocols and their accomplishment evaluation based on various mobility models.

3. LITERATURE SURVEY

Waleed Kh. Alzubaidi,et al: Nowadays WSN face security is one of the crucial dare. With development in technology with pace of time our networks becomes more unsafe to vary of various attacks. As we know we cannot provide abundant power and memory to each sensor node due this drawback unauthorized person place a malicious node in the network which could be very harmful and that is why security becomes unfeasible. The sensing technology when collaborated with managing power and wireless communication makes it fruitful. The wireless communication technology collects diverse security threats. In this article various category attacks are discussed in WSN [1].

Jyoti Neeli, et al: This article focuses how to make our routing protocol more secure and as we know after tremendous research in this domain till now it is lime light problem. In earlier times wired devices are used but with pace of time new innovation came into existence into real world which made our life so comfortable. In the same way MANET did the same way and wired devices replaced by wireless technology. A cluster is formed between various nodes and data is transmitted from one device to other node in form of packet. In this research an extreme analysis executed on security and trust communication between various nodes carried out so that black hole can not affect the data which have to send destination node. Besides this our research is also able to recognized gap between existed technology and future techniques [2].

Mahesh Kumar, et al: We can say that VANET is a special types of application of Mobile Ad-hoc Networks which able to give communications between vehicles. There are huge numbers of stuff which make VANETs prone for attackers to access our data or to control our network or can say to reduce our network performances. There are different types of attack available in which black hole attack in MANET/VANET is the most dangerous attack with the field of CN (computer networking). In this research article our main focus is to exhibit black hole attack impact on VANET AODV routing protocol by considering various networking parameters which are essential foe comparative analysis [3].

Sonia, et al: Vehicle Ad-hoc Network is endangered to various attacks. One of the chief attacks is the black hole attack which accessed all data which should be sent to destination node and in this attack malicious node sent an acknowledgement to source node that data is accessed properly by source node. In this article different types of routing protocol examined by considering malicious node in the network and after that a comparative analysis carried out which show which protocol is more endangered to the black hole attack. Out of these protocols DSR routing protocols shows best performance in regard of various networking parameters [4].

Vimal Bibhu, et al: In this paper performance analysis of the black hole attack in Vehicular Ad Hoc Network examined. In this research various types of attacks and their depth in ad hoc network carried out. End to end delay, network throughput and network load, the delay and throughput is considered for

the evaluation of attack using OPNET 14.5 modeler. The simulation setup comprises of 30 Vehicular nodes moving with constant speed of 10 meter per second [5].

Samba Sesay, et al: This article depicts logical view on ad hoc wireless networks, by considering various research challenges in ad hoc network. It begins with origin of adhoc network and various evolution phase of ad hoc network. After that a detailed analysis carried out in term of various aspects and then divided into different domain for example application in various domain, characteristics, topologies, capabilities, and design limitation of ad hoc network fully discriminate it from classical networks. Besides this article also explore wide domain of research problems such as QoS, Energy, security and many more parameters [6].

4. COMARISON

In this table there is a comparative analysis depicted executed by various researchers

Authors	Work Done	Technique Used
Waleed Kh. Alzubaidi, Shaimaa H. Shaker	Various category attacks are discussed	Wide variety of attacks in WSN and their classification mechanisms
Jyoti Neeli, N K Cauvery	How to make our routing protocol more secure	In this research an extreme analysis executed on security and trust communication between various nodes carried out so that black hole can not affect the data which have to send destination node.
Mahesh Kumar, Kuldeep Bhardwaj	Our main focus is to exhibit black hole attack impact on VANET AODV routing protocol by considering various networking parameters	Security algorithm to secure information from severe attacks
Sonia and Padmavati	Different types of routing protocol examined by considering malicious node in the network	Dynamic Source Routing Protocol
Vimal Bibhu, Kumar Roshan, Dr. Kumar Balwant Singh, Dr. Dhirendra Kumar Singh	In this research various types of attacks and their depth in ad hoc network carried out.	Black hole attack in WSN
Samba Sesay, Zongkai Yang and Jianhua	This article begins with origin of adhoc network and various evolution phase of ad hoc network.	Application in various domain, characteristics, topologies, capabilities, and design limitation of ad hoc network fully discriminate it from classical networks.

.

The main focus of research is to develop new technology which is economical as well easy to understand with optimized efficiency so that resources can be utilized efficiently. In these days with pace of time new technology came into existence at very rapid rate as compared to last decade. Above table depicts research of various researchers in various domains with diverse methods to fetch maximum output.

5. RESEARCH METHODOLOGY

Module 1

1. To Integrate a malicious node (attacker node) in AODV routing protocol.
2. Integrate Black hole attack in AODV routing protocol.
3. Calculate the Performance parameters like PDR, Throughput, Delay, Energy, and Overhead.

Module 2

1. After that, integrate a Proposed Method and Proposed Protocol to Secure AODV routing protocol.
2. Compare the Both base model and proposed model.
3. Calculate the Performance parameters like PDR, Throughput, Delay, Energy, and Overhead.

6. CONCLUSION

Security of adhoc network is one of important characteristics for its deployment. The network unsafe is more possible with the sensor nodes in abandoned environment. Wireless Sensor networks are gently enhanced used in diverse domain like military, health, environmental and commercial applications. Wireless Sensor networks are deep rooted different from conventional wireless networks as well as ad-hoc wireless networks. Security is a significant aspect for the deployment of Wireless Sensor Networks. In this paper, detailed analysis executed regarding behavior and challenges of security threats in Ad-Hoc networks with infusion finding methods. With pace of time new technology came into existence to enhance the various network parameters. To keep in mind security concern need to deploy advance protocol which can stand against severe security threat. Now day's artificial intelligence machine learning (ML) becoming very famous among researchers with IoT concept.

7. REFERENCES

[1]. Waleed Kh. Alzubaidi, Shaimaa H. Shaker, "Methods of Secure Routing Protocol in Wireless Sensor Networks", Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.3 Year 2018, 2521 – 3504

[2]. Jyoti Neeli, N K Cauvery, "Insight to Research Progress on Secure Routing in Wireless Ad hoc Network ", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[3]. Mahesh Kumar, Mr. Kuldeep Bhardwaj,"Impact of Black hole on AODV based routing in Vehicular Ad-hoc Networks", International Journal of Wired and wireless communication, Vol 4, issue 1, oct 2015.

[4]. Sonia and Padmavati,"Performace analysis of Black hole Attack on VANET'S Reactive Routing Protocols", International Journal of Computer Applications (0975- 8887) Vol. 73-No.9, July 2013

[5]. Vimal Bibhu, Kumar Roshan,"Performance analysis of Black hole Attack in VANET". International Journal Computer Network and Information security, 2012,11 pp-47-54.

[6]. S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad-hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004

[7]. C. Li, Z. Wang, and C. Yang, "Secure routing for wireless mesh networks", International Journal of Network Security, vol 13, no 2, pp. 109-120, 2011

[8]. P. Tomar, P.K. Suri, M.K. Soni, "A Comparative Study for Secure Routing in MANET", International Journal of Computer Applications, Vol.4(5), pp.17-22, 2010

[9]. M. Yu, M. Zhou and W. Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," in IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-460, 2009.

[10]. Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, NY, USA, pp. 3 – 13, 2002