Exposure and Anticipation of Black hole attack: A Literature Review

Raj Kumar Soni[1], Kailash Patidar[2], Manoj Kumar Yadav[3], Rishi Kushwah[4]

Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India

Abstract

Mobile ad hoc network (MANET) is a self-configuring infrastrucless wireless network. In this all mobile nodes behaves as a router and they can select and forward the packets. There is several routing protocol in which AODV is one of the most useful protocol for delivering the packets from source to destination. But due to the dynamic nature of the networks it is more vulnerable to severe type of security threats such as black hole, wormhole, hello flood attack , Sybil attack etc. Black hole attack is one of denial of service attack which inject false route for the transmission of packets which behaves as "freshest" or shortest route. In the case of multiple malicious nodes that work together with cooperatively, the effect will be more. This type of attack is known as cooperative black hole attack. This paper presents the review of different proposed or implemented method for the removal of malicious node from the AODV protocol also comparing it with existing methods.

Keywords— *AODV, Attacks, Mobile nodes, MANET, Security Threats.*

I. INTRODUCTION

The wireless mobile ad hoc network is widely used data communication network from the previous decades. It is self deployment, Infrastructure-less wireless network. Due to its dynamic in nature node can easily join or leave and it forms the network automatically for the transmission of packets from source to destination [1]. In such type of network each mobile nodes behaves as a router which can select the suitable or shortest path itself. Such networks provides the suitability to use for applications like conferences, assembly events, in battlefield and under disaster conditions (such as flood, fire) etc. For the transmission of packet from source to destination it uses different protocols which are classified into three categories: Table driven routing protocols, on demand routing protocols and hybrid protocol. The table driven protocols are-DSDV and OLSR, on demand protocols are AODV, DSR, TORA and hybrid protocols are ZRP. In this paper mainly AODV [5,23] protocol is discussed which is source initiated protocol. It broadcast RREQ packet to its neighbor node later transmitted further to their nearby nodes. When the RREQ message packet either reaches the destination node. It encounters a node with a route to the destination a response are entrusted. That response occurs via the transmission of a route reply (RREP) message. From the outlook of security feature of the various routing protocols wireless Ad-hoc networks are not safeguard to malicious nodes attack among which Black Hole Attack is one of them in the network along with different types of attacks. A black hole is a kind of attack in malicious nodes which implies that is has shortest and freshest route for the transmission of packets to the destination. The rest part of the paper is organized as follows: In section II describe about the AODV protocol. Section III also discuss about the Black hole attack. Section IV presents the literature of various method proposed by different researchers and Last section concludes the paper.

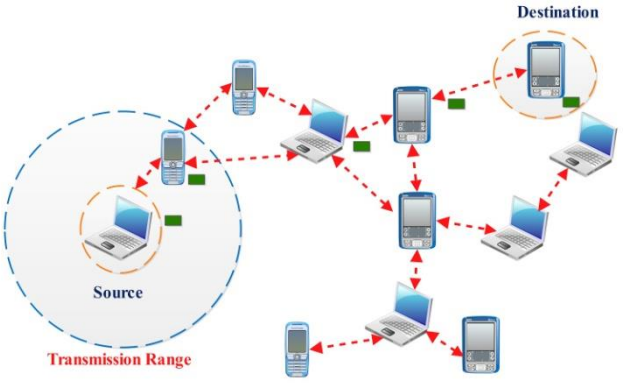

Fig.1 Mobile ad hoc networks

II. OUTLINE OF AODV ROUTING PROTOCOL

In this section we describe the overview of AODV routing protocol in mobile ad hoc network. The routing in the Ad hoc networks is a very critical task because of the absence of any central coordinator or base station and the dynamic topology.

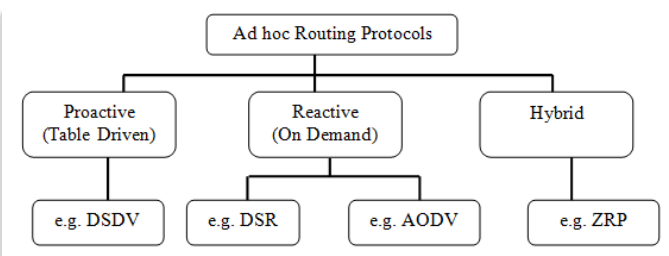

Fig. 2 Hierarchy of Routing Protocols [3]

The AODV routing protocol is a reactive routing protocol hence, paths are find when required. When a source node desires to send a message to some receiver node and it did not have a valid route to the receiver, the source node initiates a path finding process for allocating the other node. It broadcasts a route request (RREQ) packet to its nearby nodes, later transmitted further to their nearby nodes. This process continues to the extent up to which the receiver or an intermediate node with a "fresh enough" route to the destination is located. When the RREQ message packet either reaches the destination node or encounters a node with a route to the destination a response is entrusted. That response occurs via the transmission of a route reply (RREP) message. In case if a node realizes that the route is damaged or broken it transmits a route error (RERR) message to the source [2]. Figure 3 below shows the working of AODV routing protocol.

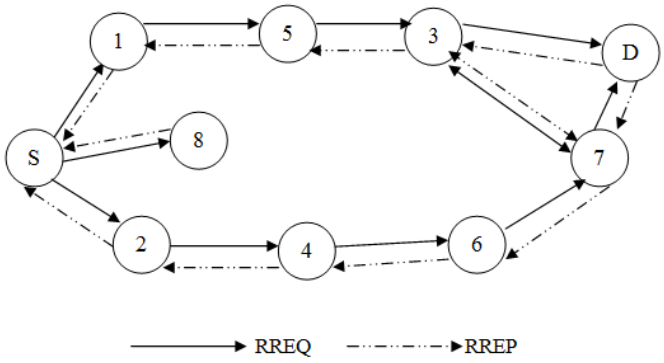

Fig. 3 Flow of Control Messages

M.Sheik Dawood et al [4] proposed the modified QoS enhanced base station controlled dynamic clustering protocol for wireless sensor networks to decreases the energy consumption of node. The simulation results show the better energy consumption is achieved by the proposed protocol when compared to the conventional techniques.

Babak et al [5] proposed an algorithm which makes healthier use of energy and bandwidth which are two restrictions in wireless sensor networks. In the algorithm mobile agent is used to cluster the network and also create the tour to attain collected data from each cluster-head and deliver it back to the sink node. With suitable parameters set, simulation shows that the proposed algorithm exhibits better performance than original direct diffusion in terms of energy consumption [6].

J.Preetheswari et al [7] developed an effective routing mechanism that can with high probability; evade the black hole formed by this attack. The Purely Random Propagation (PRP) algorithm developed produces randomized dispersive routes so that the routes taken by the distribution of different packets changes over time. Besides arbitrariness, the generated routes are also highly dispersive and energy proficient, making them quite capable of bypassing black hole. In addition, the energy constraint is highly optimized in the entire routing method leading to minimal energy consumption. Widespread simulations are conducted to explore the security and energy performance of our mechanism.

Neeraj Kumar et al [8] proposed a secure and energy proficient data diffusion protocol for WSN. A routing metric is defined to prefer the best route from the existing routes. These metric guides those routes to be preferred that consume less energy. Furthermore, for secure data diffusion, a session key is renowned between unlike parties to be communicated. This session key is then used for secure communication between nodes for data diffusion. It is found that the proposed protocol is moderately effective in comparison to the existing protocols with respect to these metrics.

Zhu et al. [9] proposed an interleaved hop-by-hop au- thentication scheme to prevent injection of false data into sensor networks. The proposal makes sure that the BS can detect a false report when no more than a certain number of nodes are compromised.

Przydatek et al. [10] proposed SIA, a framework for secure information aggregation in WSNs which makes use of random sampling strategies for allowing user to infer about the legitimacy of a value. Other efforts have focused on more specific types of attacks.

Yong-ki et al. [11] worked on a new approach for energy efficient data aggregation in sensor networks. A sensor network is self possessed of a huge amount of sensor nodes, which are supply constraints, like limited power. An usual notion to collect data by a sink node is to transmit data from sensor nodes to the sink node by multi-hop. It raised two problems first is the hotspot difficulty, in which the sensor nodes closer to the sink run out of energy nearer than other nodes. As the result, the network lost its service ability, despite of a large amount of residual energy of the other nodes. The next one is that the system generates needless traffic during data transmission for choosing a proper data-sending path. To resolves the problems, authors, propose a new energy balanced and efficient data aggregation scheme for WSNs, called designated path (DP) scheme.

Arabi et al. [12] proposed HERF: A hybrid energy efficient routing using a fuzzy method in Wireless Sensor Networks. Authors work giving attention on Data broadcasting is a significant task performed by WSNs. The algorithms of this system depend on a number of factors such as application areas, practice circumstance, power and cumulative factors. With respect to these parameters, various algorithms are recommended. An algorithm for hybrid energy efficient routing in wireless sensor networks, which used two algorithms, i.e. EF-Tree (Earliest-First Tree) and SID (Source-Initiated Dissemination) to publicize data and utilizes a fuzzy method to choose group head and to knob between two methods SID and EF-Tree.

M. Nivedita et al. [13] Proposed two keys based method were used. One of the keys is the network-wide key embedded into the nodes prior to their deployment and the other key is the dynamic key. The dynamic key encrypts the message that was primarily encrypted by network-wide key which is a compromised key. Hence, the possibility of attacks to occur is more because the compromised key is used in overall encryption process. Also, this scheme consumes significant amount of energy and memory because the encryption with multiple keys become computationally high.

Zhu et al. [14] proposed a key management protocol for sensor networks designed to support in network processing. LEAP solves the problem of key distribution and restricts the impact of a compromised node to the network. LEAP uses four types of keys for each node and communication type. Main drawback of LEAP is the excessive number of messages that must be exchanged during the establishment of keys, thus resulting in the increase of communication cost and energy consumption and limiting the network scalability.

III. ROUTING TECHNIQUES AND SECURITY ATTACK

The efficiency of energy can be improved using some algorithms. That route the data as per network and data communication systems. In this we will some of the energy efficient routing protocols which will be discussed which are LEACH (Low Energy Adaptive Clustering Hierarchy), PEGASIS (Power Efficient Gathering in Sensor Info. Systems) and TEEN (Threshold Sensitive Energy Efficient Sensor Network) etc.

LEACH:
Low Energy Adaptive Clustering Hierarchy (LEACH) is a clustering based protocol that uses a randomized rotation of local cluster base stations [15]. LEACH is one of the most popular distributed cluster based routing protocols in WSNs. LEACH is the first and most popular energy efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption and also to increases the lifetime of the network.

PEGASIS
Power-efficient Gathering in Sensor Information Systems [16] is a greedy chain-based power efficient algorithm. Also, PEGASIS is based on LEACH. The key characteristics of PEGASIS are

- The Base Station is preset at long distances from the sensor nodes.
- The sensor nodes are identical and energy constrained with consistent energy.
- No mobility of sensor nodes.

PEGASIS is based on two ideas that are chaining and data fusion. In PEGASIS every node can take twirl of being a leader of the chain where the chain can be created using greedy algorithms that are organized by the sensor nodes. PEGASIS assumes that sensor nodes have a global understanding of the network nodes are motionless (no alliance of sensor nodes) and nodes have locality of information about all other nodes. PEGASIS performs data fusion excluding the end nodes in the chain. PEGASIS better than LEACH by removing the transparency of cluster formation decreases the sum of distances that non leader node have to broadcast less the number of transmissions and receives all nodes and use only one transmission to the BS per round. PEGASIS has the identical problems that LEACH suffers from. Also the PEGASIS does not scale cannot be applied to sensor network where global knowledge of the network is not simple to get. Power Efficient Gathering in Sensor Information Systems (PEGASIS) is an enhancement of the LEACH protocol. Rather than designing multiple clusters it makes chains of sensor nodes so that each and every node transmits and receives from a neighbourhood and only one node is selected from that chain to transmit to the base station. Collected data transfer from node to node, amassed and eventually sent to the base station.

TEEN
Threshold sensitive energy efficient sensor network protocol is used for precipitous changes in the sensed attributes in the network. It uses a data centric mechanism and makes clusters in a hierarchical manner. Two threshold values are transmits to the nodes: hard threshold and soft threshold. The hard threshold is the least promising value of an attribute. Sensor nodes mail data to the cluster head only if they found the sensed value is higher than the hard threshold.
If sensor nodes found that the sensed value is less than the feature value of threshold than they do not send the data to the cluster head. By this way only relative data is send by the sensor nodes. Further; when sensor node again sense value greater than the hard threshold value than they check the difference between current and earlier value with soft threshold. If the dissimilarity is again greater than the soft threshold than the sensor nodes will send recent sensed data to the cluster head. This process will remove encumber from the cluster head [17]

Security Threats in WSN
The WSN is more vulnerable to security threats and it is very necessary to guard our networks from these attacks which are- denial of service, wormhole, hello flood, sinkhole attack.

DENIAL OF SERVICE ATTACK:
Denial of Service (DoS) attack is means that not only for the adversary's attempt to subvert, disrupt, or destroy a sensor network, but also for any event that diminishes a sensor network's capability to provide a service [3].In WSNs, several types of Denial of Service attacks in different layers might be performed i.e. at physical layer, the Denial of Service attacks could be jamming and tampering at link layer, confrontation, fatigue, unfairness at network layer, neglect and voracity homing, misdirection and black holes at transport layer this attack could be performed by malicious flooding and resynchronizations [18,23].

SYBIL ATTACK:
It is defined as a malicious device illegitimately taking on number of identities. In this Sybil attack, a single sensor node i.e. a malicious sensor device will appear to be a set of sensor devices and it will forward the incorrect message to a sensor node in the network which definitely decreases the normal performance of fault tolerant such as distributed storage, disparity and paths. This incorrect message may be any things [19], which may include the position of sensor nodes, strength; the generation of node which is not actually exists.

WORMHOLE ATTACK:
In wormhole attack [20], a pair of attackers forms "tunnels" to transfer the data packets and replays them into the network.

This attack has an incredible effect on wireless networks particularly against routing protocols. Routing method can be baffled and interrupt when routing control messages are tunnelled. It could be formed among the two colluding attackers is referred as wormhole.

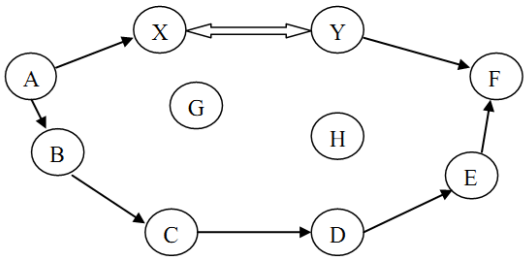

Fig.2 Wormhole Attack

HELLO FLOOD ATTACK:

In this, HELLO packets will have high radio transmission range and these are used as weapons in WSN. This processing power sends HELLO packets to a number of sensor nodes which are deployed in a large area within a Wireless Sensor Network. The sensor devices are thus persuaded that the adversary is their neighboring nodes. As a result of this, while forwarding the messages to the base station, the victim sensor nodes try to go through the attacker as they are aware, that it is their neighbours and are spoofed by the attacker [22].

IV. CONCLUSION

The wireless sensor network nodes has limited battery energy and the nodes are also more vulnerable to security attack over the network while many researcher has proposed and implemented different methods and its countermeasures to prevent the network from threats also to improve the battery lifetime but sometimes the it has affected by some other factors so in future the author must need to focus the advancement in battery power and also provide better fault tolerance also protect the sensor network from severe security threats.

REFERENCES

[1] Adil Bashir, Ajaz Hussain Mir, “An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network”, International Conference on Advanced Electronic Systems (ICAES) , 2013 in proceeding of IEEE xplore.

[2] Sudharsan Omprakash, Giridharan Nanthagopal, Santosh Kumar Omprakash, “A secured energy efficient clustering and data aggregation protocol for wireless sensor network”, American Journal of Computation, Communication and Control 2014; 1(1): 18-23 published online April 20, 2014

[3] Z. Tanveer, Z. Albert, “Security Issues in wireless sensor networks”, IEEE 2006.

[4] M.Sheik Dawood, S.Sadasivam, G.Athisha, “Energy Efficient Wireless Sensor Networks based on
QoS Enhanced Base Station controlled Dynamic Clustering Protocol.

[5] BabakNikmard and Salman Taherizadeh, “Using mobile agent in clustering method for energy consumption in wireless sensor network”, International Conference on Computer and Communication Technology (ICCCT), pp.153-158, 2010.

[6] Ali K., Neogy S., and Das P.K., “Optimal Energy-Based Clustering with GPS-Enabled Sensor Nodes”, Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM), pp.13-18, 2010

[7] J.Preetheswari, J. Mark Jain, “ Optimized Secure Data Delivery based on Randomized Routing in Wireless Sensor Networks”, International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012)

[8] Neeraj Kumar, Manoj Kumar, and R. B. Patel, “A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks”, International Journal of Network Security, Vol.15, No.6, PP.490 {500, Nov. 2013}

[9] S. Zhu, S. Setia, and S. Jajodia, “An interleaved hop- by-hop authentication scheme for filtering of injected false data in sensor networks," IEEE Symposium on Security and Privacy, pp. 259-271, 2004.

[10] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure information aggregation in sensor networks," ACM SenSys 2003, Nov. 2003.

[11] Yanwei Wu, Xiang-yang Li, Mo Li, Wei Lou, Energy-Efficient Wake- Up Scheduling for Data Collection and Aggregation, Parallel and Distributed Systems, IEEE Transactions on , vol.21, no.2, pp.275,287, Feb. 2010.

[12] Arabi, Z., HERF: A hybrid energy efficient routing using a fuzzy method in Wireless Sensor Networks, Intelligent and Advanced Systems (ICIAS), 2010 International Conference on , vol., no., pp.1,6, 15-17 June 2010.
[13] M. Nivedita, "A Dynamic Cryptographic Algorithm To Provide Nodal Level Security In Wireless Sensor Network", International Conference on Innovative Computing and Communication, Asia- IEEE Computer Society-2010
[14] S. Zhu, S. Setia and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks"s, 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., USA, October 2003
[15] Alakesh Braman, Umapathi G. R, "A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks: A survey", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014
[16] Fan Wu," incentive-compatible opportunistic routing for wireless networks", mobicom'08, September 14–19, 2008, San Francisco,California, USA 2008
[17] Naveen Sharma and Anand Nayyar, "A Comprehensive Review of Cluster Based Energy Efficient Routing Protocols for Wireless Sensor Networks", International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 1, January 2014 ISSN 2319-4847
[18] David R. Raymond and Scott F. Midkiff, (2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.
[19] D.G. Anand, H. G. Chandrakanth, M. N. Giriprasad, "THREATS & ISSUES IN WIRELESS SENSOR NETWORKS", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 1, Jan-Feb 2012, pp.911-916
[20] Nishant Sharma, Upinderpal Singh, "A Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 ISSN: 2277 128X.
[21] Jitendra Sheetlani, Harsh Pratap Singh, Nagesh Salimath, K Murali Gopal, "Design and Implementation of an Algorithm for Mitigating the Congestion in Mobile Ad Hoc Network", International Journal on Emerging Technologies, Vol-10, Issue-3, 2019. Pp. 472-479
[22] Chris Karlof, David Wagner, (2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.
[23] Harsh Pratap Singh, Rashmi Singh, "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol", International Conference on Electronics and Communication Systems (ICECS), 2014.