International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 05, May 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

AN ECC BASED ROUTING ALGORITHM FOR DETECTION AND AVOIDANCE OF BLACKHOLE & WORMHOLE ATTACK IN MANET

Christophel selvi L,[1] Caroline Jebakumari S[2]

[1]M.E - Communication Systems, [2]Assistant Professor Dept of ECE

Easwari Engineering College, Chennai.

ABSTRACT

MANET is a hierarchy of decentralized nodes and dynamically changing network topologies where the nodes are in mobile conditions for the dissemination of data. But, MANET is liable to attacks such as Wormhole, Grayhole, and Sinkhole attack where the performance of entire network is degraded. Hence it is necessary to provide security to the network as the data's transferred through the attack prone network may be outraged. A fictitious node mechanism is implemented by the creation of imaginary nodes using T-OLSR routing protocol. In order to provide security to the network ECC (Elliptic Curve Cryptography) algorithm is implemented. The reason behind the use of T-OLSR algorithm is better performance, less delay and minimum time utilization for packet dispatching when compared with Chord algorithm.

Keywords: Security, Cluster head agents, Malicious nodes, Fictitious node, T-OLSR, ECC.

I. INTRODUCTION

Adhoc networks are defined as the category of wireless networks that utilize multihop relaying and are capable of operating without a fixed infrastructure. The absence of any central coordinator or base station makes the routing a complex one compared to cellular networks .The presence of base station in cellular network simplifies routing and resource management as the routing decisions are made based on fixed infrastructure. But in Adhoc networks the routing and resource management are done in a distributed manner in which all nodes coordinate to enable communication among themselves which require each node to be intelligent so that it can function both as network host from transmitting and receiving data as a network router for routing packets from source to destination[10].

The presence of mobility implies that links make and break often in an inter-deterministic fashion. Routing protocols such as distance vector and link based routing is not designed for wireless networks it is still applied for radio networks. These routing protocols are unable to catch up frequent link changes in Adhoc wireless network resulting in poor convergence and very low communication throughput. Hence these protocols are to be modified [11].

Mobile Adhoc networks are prone to various types of attacks such as replay attack, masquerade attack, wormhole attack, Gray Hole Attack, Denial of service, Eavesdropping, out of which Blackhole attack is the

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

common one. Malicious node capture the packet and does not forward them but advertise itself as having the shortest path to the packet which it needs to intercept.if more than one malicious nodes occurs as group it is known as blackhole attack. In this paper a mechanism for identifying the Blackhole attack is proposed which works based on the cooperative cluster head mechanism which generates an alert notification to other nodes which improves the performance of network in terms of packet delivery ratio, throughput and end to end delay.

The rest of this paper is organized as follows section 2 describes about the related work, section 3 describes about the operation of T-OLSR routing protocol and ECC algorithm, section 4 describes about modules implemented in this project, section 5 about the simulation metric and its discussion in section 6, section 7 describes about conclusion and future work.

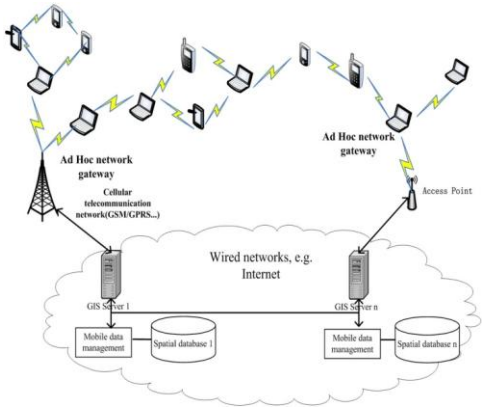

Figure 1.1 Adhoc Network Architecture

II. SIMILAR WORKS

Jay Dip Sen, Sripad Koilakonda [4] have discussed in their paper about the research areas in Adhoc network community. Here AODV works based on the routing information table along with the information obtained from the cached and current routing table. In order to avoid Blackhole attack securing the routing layer is more important. In addition to protect the routing layer attack can be prevented by detecting the misbehaving nodes and giving an error report to source node as false positive. In this paper when the route reply packet is obtained from the intermediate node, source gives another route request packet to intermediate node for ensuring that the path exists.

Yanzhi Ren, Mooi Chao Chuah [5] have discussed in their paper about the surveillance when selective dropping of the packet occur. This concept uses DTN (Delay Tolerant Networks) that is designed to operate over extreme distances such as space communication or interplanetary scales. But DTN seemed to be a failure concept as there cannot be sparse network to act as monitoring nodes. To detect the abnormal behavior of the nodes overhead packets and energy consumption a transitive property is considered which is used to encounter the nodes used in DTN. This method prevents the hacker from non-existence and cannot cope up with packet dropping which is a drawback of this method.

H.A Esmaili, Hossein Ghararee[3] have encountered that malicious nodes wrongly advertise that it has the shortest path to reach the destination but does not forward to them instead it drops the packet leading to selfish behavior. Wenkee Lee,Yi-An Huang have used IDS(Intrusion detection system) to collect a systematic approach

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

about the data nodes for detecting anamoly nodes based on correlating the features available within the networks . This paper uses cluster based detection scheme where periodically every node in the network is updated as cluster agent. Smita Karamakar present a study of voroni and triangular oriented diagram that is used to calculate the size of a coverage hole. Depending on this coverage area the nodes are assigned with the cluster heads. A straightforward algorithm is proposed which detects when the sensor node is dead it assumes that there is no sensor node in that area and it assumes that region has a hole. Tarun Varshney proposed mechanism to prevent Blackhole attack by slightly modifying the AODV called watchdog-AODV that detects normalized routing overhead and generates a new route to the source and isolates the malicious nodes during the route discovery process.

Tamilselvan et al [5] proposed a time based threshold detection scheme where a timer is set for collecting the request from other nodes after establishing the path. This will be stored in the Collect route reply table (CRRT) where the validity is checked based on the arrival time of the first packet and threshold value. This method remains a drawback as overhead is high when compared with AODV. In order to overcome the above drawbacks a new modified chord algorithm is proposed which works based on the update information in the routing table.

III. ALGORITHMS IMPLEMENTED

3.1 T-OLSR

Trusted Optimized Link State Routing protocol is a proactive link state routing protocol. The protocol inherits the stability of link state routing algorithm. Due to its proactive nature it has the ability of providing the routes needed immediately. In a pure link state protocol all the links with neighbor are flooded and declared in the entire network. OLSR protocol is an optimization of pure link state protocol for mobile Adhoc networks. First it reduces the size of control packets; instead of all links it shares only within the subsets who are its multipoint selectors.

3.2 MULTIPOINT RELAYS

The idea of multipoint relay is to minimize the flooding of Broadcast packets in the network by reducing duplicate transmissions in the same region. Each node in the networks selects a set of nodes in its neighborhood, which transmits its packets. This set of selected neighbor nodes is called the Multipoint relays (MPRs) of that node. The neighbors of any nodes N which are not in its MPR sets read and process the packet but do not retransmit the broadcast packet received from Node N . For this purpose, each node maintains set of its neighbors which are called the MPR selectors of node. Every broadcast message coming from these MPR selectors of a node is assumed to be retransmitted by that node. This set can change over time which is indicated by the selectors nodes in their HELLO messages.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

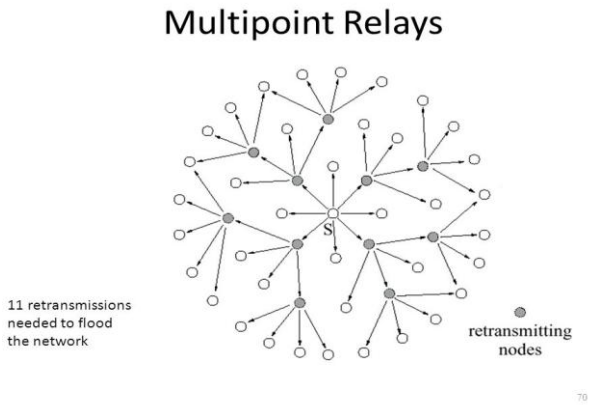

Figure 3.1 Multipoint Relay

3.3 MULTIPOINT RELAY SELECTION

The interval between the transmission of two TC messages depends upon whether the MPR selector set is changed or not. Since the last TC message transmitted. When a change occurs in the MPR selectors set , the next TC message may be sent either that the scheduled time, but after some pre specified minimum interval ,starting from the time the last TC message was sent.

Upon receipt of TC message, the following proposed procedure may be executed to record the information in the topology table,

1. If there exist some entry in the topology table whose last hop address corresponds to the originator address of the TC message and the MPR selector sequence number in that entry is greater than the sequence number in the received message. Then no further processing of this TC message is done and it is silently discarded(Case: packet received out of order)
2. If there exist some entry in the topology table whose last hop address corresponds to the originator address of the TC message and the MPR selector sequence number in that entry is smaller than the sequence number in the received message, then the topology entry is removed.
3. For each of the MPR selector address received in the TC message :

- If there exist some entry in the topology table whose destination address and the last hop address of the entry corresponds to that originating address of the TC message, then the holding time of that entry is refreshed.
- Otherwise new topology entry is recorded in the topology table.

3.4 PROTOCOL FUNCTIONING

Neighbor Sensing

- OLSR protocol relies on the selection of multipoint relays, and calculates its routes to all known destinations through its nodes. i.e MPR nodes are selected as intermediate nodes in the Path. To implement this scheme, each node in the network periodically broadcast the information about its one-hop neighbors which have selected it as a multipoint relay. Multipoint relays of given node are declared in the subsequent HELLOs transmitted by this node. So that the information reaches the multipoint relays themselves. The multipoint

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

relay set is re-calculated when, A change in the neighborhood is detected when either a bi-directional link with a neighbor is failed. Or a new neighbor with a bi-directional link is added: or

- A change in the two-hop neighbors set with bi-directional link is detected.

3.5. ECC (Elliptic Curve Cryptography)

Majority of public key crypto systems use either integer or polynomial arithmetic with very large numbers/polynomials. This imposes a significant load in storing and processing keys and messages. An alternative is to use an Elliptic curve which offers same security with smaller bit sizes.

IV. FINITE ELLIPTIC CURVES

Elliptic curve cryptography uses curves whose variables & coefficients are finite. ECC have two families commonly used prime curves $E_p(a,b)$ defined over Z_p binary curves $E_{2m}(a,b)$ defined over $GF(2^n)$

V.ECC Encryption/Decryption

Each user chooses private key $n_A<n$ and computes public key

$P_A= n_A*G$

To encrypt P_m: $C_m =\{ k G, P_m+ K P_A\} ,K$

To decrypt C_m compute

$P_m+ KP_A- n_A(KG) = P_m+ k(n_AG-n_A) (KG) = P_m$

VI. MODULES IMPLEMENTED

A modular design reduces complexity, facilities change (a critical aspect of software maintainability) and results in easier implementation by encouraging parallel development of different part of system. To identify the nodes that are malicious during Blackhole attack several modules have been implemented in this project. The modules are listed as follows

- Node Construction
- Data Transmission Based On DTN
- Identification Of Selfish/Malicious Node Based False + ve or –ve
- Data transmission
- Attack detection and avoidance
- Performance analysis

VII. PERFORMANCE ANALYSES

6.1 Without T-OLSR& With T-OLSR

The following graph shows the performance in terms of throughput, packet delivery ratio , average delay, delay for the given number of nodes. From the graph it can be observed that without using T-OLSR performance is very less when compared with using T-OLSR.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

6.1.1 Throughput

In data transmission, network throughput is the amount of data moved successfully from one place to another in a given time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps).

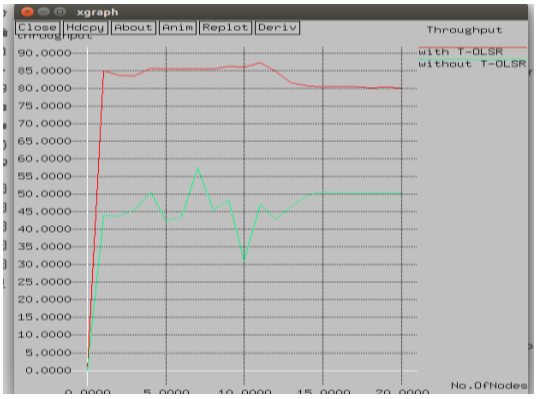

Figure 6.1 Throughput

6.1.2 Delay

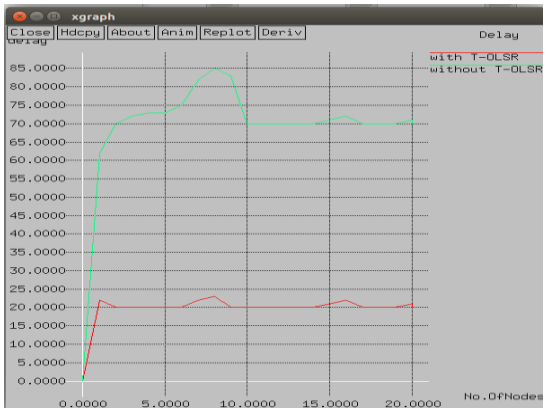

Figure 6.2 Delay

6.1.3 Average Delay

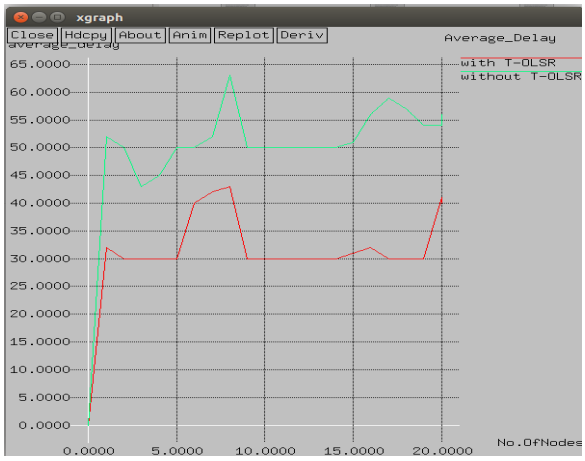

Figure 6.3 Average Delay

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

6.1.4 Packet Delivery Ratio

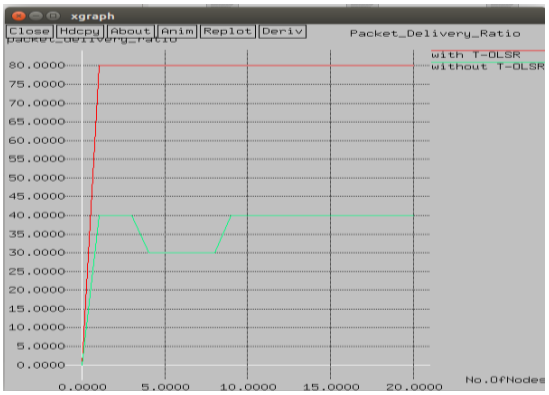

Figure 6.4 Packet delivery ratio

VIII. CONCLUSION & FUTURE WORK

Thus the security issues in MANET have been explained in detailed manner. There might be a numerous solution in the past for securing the routing protocol, some results work well in detecting the attacks with a single node. In this paper we have deployed 28 nodes and simulated the same scenario. In future the number of fictitious node is reduced in order to obtain the optimal solution better than the result obtained.

REFERENCES

[1] Lata Ragha, Vaishali Gaikwad "Security Agents for Detecting and Avoiding Cooperative Blackhole Attacks in MANET" @ 2015 IEEE.

[2] Chandni Garg, Preeti Sharma, Prashant Rewagad" A Literature Survey of Black Hole Attack on AODV Routing Protocol," International Journal of advancement in electronics and computer engineering (IJAECE) Volume 1, Issue 6, Sep 2012.

[3] H.A. Esmaili, , Hossein gharaee, M.R. Khalili Shoja "Performance Analysis of AODV under Blackhole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, pp. 49-52, 2011.

[4] J.Koilakonda Sen, Ukil, A., "A Mechanism for Detecting of Cooperative Blackhole Attack in Mobile Ad Hoc Networks", Second International Conference on Intelligent Systems, Modelling and Simulation (ISMS), pp.338-343, Jan. 2011.

[5] Mooi Choo Chuah, Jie Yang, Yanzhi Ren Yingying Chen, "Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording", IEEE Wireless Communications, Vol. - 11, 2010.

[6] Y. Chen, M. C. Chuah, J. Yang, and Y. Ren, "Mouton: Detecting malicious nodes in disruption-tolerant networks," in *WCNC 2010*, 2010.

[7] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issue, Vol. 2, pp 54–59, 2009.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[8] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting Blackhole attack on AODV based mobile ad-hoc networks by dynamic learning method, "International Journal of Network Security, pp. 338–346, 2007.

[9] B.S.Manoj , C.Sivaramamurthy "Adhoc wireless networks",2007

[10] V.Cahill, S. Farrell Delay and Disruption Tolerant Networking. Artech House, 2006.

[11] M. Al-Shurman, S. Park, S-M. Yoo, "Black Hole Attack in Mobile Ad-Hoc Networks," ACM Southeast Regional Conf. 2004.

[12] Chen J, Guan Y, Sun B, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.