ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Honeypot-based Defense System Design

[1] N.Priya, [2] K.Naga Teja, [3] M.Anjay,
[1] Asst Professor, Department of CSE, BIHER,
[2] [3] UG Student, Department of CSE, BIHER,Chennai,TN,INDIA

Abstract: ***In mobile ad hoc network (MANET), energy consumption is one among the foremost vital restrictions that deteriorate the performance of the whole network. Multi-path routing is better than the single path routing in ad hoc networks, because multi path routing allows the establishment of multiple path between a single source and single destination node. This project presents a new approach of energy efficient secure multipath hybrid (EESM-hybrid) routing protocol for MANET based on both AODV and AOMDV protocol is modified and converted to work on multiple path .Differing types of routing protocols planned over the years with minimal management overhead and network resources. Hybrid protocol(both AODV & AOMDV) is well-liked routing protocol among others. It is a loop free, no centralized authority, single path, On-demand routing protocol and its performance is superior than different routing protocols in MANET.***

Keywords: Honeypot, hacking, security, forensic analysis of honeypots, network.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless devices moving in seemingly random directions[1,2,3] and communicating with one another without the aid of an established infrastructure. Communicating nodes in a Mobile Ad hoc Network usually seek the help of other intermediate nodes to establish communication channels. Thus, the communication may be via multiple intermediate nodes from source to destination. Topology[4,5] changes occur unpredictably. Topology control is needed to determine appropriate topology in adhoc network which saves energy, reduce interference between nodes and extends the lifetime of the network. Based on connectivity, efficiency of energy, robustness to mobility and throughput the quality of topology is determined. High level routing protocols[6,7] are implemented over a suitable topology .All nodes connected in a network must act as routers to have accurate delivery of data packets. Routes contain links which is the connection between two nodes. The route quality is influenced by change in link quality. A varying link route does not produce good results. The network layer has received a notice when working on Mobile Adhoc Network. Therefore plenty of routing protocols in such network with different objectives and with different specific needs have been proposed. As a matter of fact, the two vital operations at the network layer are data forwarding and routing[8,9,10]. Data forwarding controls how packets are taken from one link and put on another. Routing finds out the path which the packet must follow to reach the destination from the source. Routing protocols can be divided into single path and muItipath based on the nwnber of routes discovered . Single path protocols learn routes and select a single best route to reach each destination. These protocols are unable to balance traffic load . Single route simplify the routing table and packet forwarding but it has many disadvantages. Even though additional network resources may be available, using a single path, it is difficult to respond to a large burst in traffic. If the path fails a new route discovery must be initiated resulting in significant delay and packet loss[11,12]. Multi path protocols learn routes and select more than one path to reach the destination. They are better for load balancing. Multipath routing improves communication efficiency and promotes Quality of Service by utilizing different paths simultaneously [5]. Also they are more reliable, robust and consequently reduces control overhead, enhances data transmission rate, the network bandwidth is increased and the energy is saved . Contributions in our solution are as follows.

1. A multipath proactive source routing protocol is used as each node has complete knowledge of how to route data to all nodes in the network at any time. Based on the number of paths available to reach destination, the packets can be divided and sent simultaneously to destination.

2. When the data packets are forwarded towards destination the intermediate nodes can adjust the route information carried by them. Furthermore, as these packets are forwarded along the new route, such updated information is propagated upstream quickly without any additional overhead. As a result, all upstream nodes learn about the new route at a rate much faster than via periodic route exchanges. Opportunistic data forwarding[13,14,15] is taken to another level by allowing nodes that are not listed as intermediate forwarders to retransmit data if they believe certain packets are missing.

Malicious nodes may become part of actively used routes and disrupt network operation. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. In this paper, we focus on a special type of denial of service attack due to RREQ[16,17,18] flooding attack. In this type of attack, those malicious nodes

behave like the normal nodes in all aspects except that they initiate frequent RREQ control packet floods. This type of attack is hard to detect since any normal node with frequently broken routes could legitimately initiate frequent route discoveries. One or more malicious nodes flooding the MANET with RREQ control packets related to bogus route discoveries can cause a sharp drop in network throughout.

II. ENERGY AWARE ROUTING IN MOBILE ADHOC NETWORK

Wireless mobile devices are useful if they can be used anywhere. But we have limited battery power of using it, Therefore, in wireless communication; one of the most challenging problems is power management. Several energy aware routing protocols have been developed. Most of these routing protocols aim to minimize the energy consumed per packet needed to deliver this packet to its destination. Some of the more sophisticated routing algorithms associate a cost with routing through a node with low power reserve. Other routing protocols aim to maximize the network lifetime. All previous protocols are using single path to distribute data traffic through the network. The routing protocols, described previously are based on the single path routing[19,20] between a source and a destination. However, in a reasonably well-connected network, there may exist several paths between a source-destination pair. The concept of multipath routing is to give the source node a choice at any given time of multiple paths to a particular destination by taking advantage of the connectivity redundancy of the underlying network. The multiple paths may be used alternately, namely, traffic taking one path at a time, or they may be used multiple paths simultaneously .Multi-path routing consists of three components: route discovery, route maintenance, and traffic distribution among multiple paths.

A. Route Discovery: It finds multiple routes between a source and destination nodes. Multipath routing protocols may be node disjoint (no common nodes), link disjoint (no common links), or non-disjoint routes. Non-disjoint routes may have lower aggregate resources than disjoint routes for the reason that non-disjoint routes share links and nodes. Disjoint routes provide higher fault-tolerance.

B. Route Maintenance: It finds and repairs the broken paths.

C. Traffic Allocation: The traffic allocation strategy is used to deal with how the data is distributed amongst the paths.

III. DENIAL OF SERVICE ATTACK DUE TO ROUTE REQUEST (RREQ) FLOODING

The Route Request (RREQ) Flooding Attack is a kind of denial-of-service attack, which aims to flood the network with a large number of RREQs to the destinations in the network. In this attack, the malicious node will generate a huge number of RREQs, may be hundreds or thousands of RREQs, into the network until the network is saturated with RREQs and unable to transmit data packets. Many different reactive (on-demand) dynamic routing protocols proposed for MANETs can suffer from this type of attack. On-demand routing protocol, uses a route discovery process to obtain a route when a node want to send a data packet to a destination for which it does not information about the route. The route discovery works by broadcasting the network with route request (RREQ) control packets. A node that receives a RREQ rebroadcasts it, unless it has information about another neighbor, intermediate node or it has a route information to the destination indicated in the RREQ. If the received RREQ is a duplicate or it has a same sequence number, it will be dropped. If a node has the route information because it is the destination then it replies to the RREQ with a route reply (RREP) [21,22] packet that is routed back to the original sender of the RREQ. In an ad hoc wireless network energy and traffic load are the two major elements for research, the RREQ packets used for route discoveries may consume more bandwidth than the data packets. Malicious nodes could exploit this weakness of routing protocols. Attackers can initiate much more REEQ control packets than the normal nodes to consume network resource. Since control packets are given higher priority over data packets in transmitting, In this situation, valid communication cannot be kept and normal network nodes cannot be served, then it leads to a type of denial-of-service attack. In some on-demand protocols, for example AODV, a malicious node can override the restriction put by RREQ_ RA TELIMIT (limit of initiating / forwarding RREQs) by increasing it or disabling it. A node can do so because of its self-control over its parameters. The default value for the RREQ_ RATELIMIT is 10 as proposed by RFC 3561. A compromised node may choose to set the value of parameter RREQ_RATELIMIT to a very high number. This allows it to flood the network with fake RREQs and leads to a type of Denial of service attack. In this type of Denial of service attack a non-malicious node cannot fairly serve other nodes due to the network load imposed by the fake RREQs. This will not only lead to the exhaustion of the network resources like memory (routing table entries), but also lead to the wastage of bandwidth and the wastage of nodes' processing time.

SYSTEM ANALYSIS

EXISTING SYSTEM

A mobile ad-hoc network or MANET is a collection of mobile nodes sharing a wireless channel without any centralized control or established communication backbone. They have no fixed routers with all nodes capable of movement and arbitrarily dynamic. These nodes can act as both end systems and routers at the same time. When acting as routers, they discover and maintain routes to other nodes in the network. The topology of the ad-hoc network depends on the transmission power of the nodes and the location of the mobile nodes, which may change from time to time . One of the main problems in ad-hoc networking is the efficient delivery of data packets to the mobile nodes where the topology is not pre-determined nor does the network have centralized control. Hence, due to the frequently changing topology, routing in ad-hoc networks can be viewed as a challenge.

A Mobile Ad-hoc Network (MANET) is a dynamic wireless network that can be formed without the need for any pre-existing infrastructure in which each node can act as a router. One of the main challenges of MANET is the design of robust routing algorithms that adapt to the frequent and randomly changing network topology. A variety of routing protocols have been proposed and several of them have been extensively simulated or implemented as well. In the existing comparision and evaluate the performance of two types of On- demand routing protocols- Ad-hoc On-demand Distance Vector (AODV) routing protocol, which is unipath and Adhoc On-demand Multipath Distance Vector (AOMDV) routing protocol.

DISADVANTAGES

- **Spends a lot of time planning paths that will never get used.**
- **Heavily reliant on fast collision checking.**
- **Bandwidth is wasted.**
- **Increasing network congestion.**

PROPOSED SYSTEM

EESM-hybrid routing protocol work for Ad-hoc networks. It stands for ENERGY EFFICIENT SECURE MULTIPATH HYBRID PROTOCOL. Here in this comparison distance and mobility plays an important role,.EESM-HYBRID protocols have some desirable properties of providing bandwidth and energy efficiency. We can say that with respect to existing protocols, in EESM-HYBRID more bandwidth and energy (required for transmission in each mobile node) can be used for the transmission of data messages. Most importantly:

1. The rate of control message generation is determined and optimized according to the mobility rate of each node individually.
2. Due to the “distance effect” the number of hops (radius from the moving node) it will be allowed to travel in the network before being discarded will only depend on the relative (geographic) distance between the moving node and the location tables being updated.

EESM-HYBRID protocol provide loop-free path, since each data message propagates away from its source in a specific direction. EESM-HYBRID protocol is also adaptive to mobility, since the frequency with which the location information is disseminated depends on the mobility rate.

The RATE_LIMIT parameter denotes the number of RREQs that can be accepted and processed as normal per unit time by a node. Each node monitors the route requests it receives and maintains a count of RREQs received for each RREQ ongmator during a preset time period. Whenever a RREQ packet is received, a check is performed. If the rate of this RREQ originator is below the RATE_LIMIT, the RREQ packet is processed as normal. The BLACKLIST_LIMIT parameter is used to specify a value that aids in determining whether a node is acting malicious or not. If the number of RREQs originated by a node per unit time exceeds the value of BLACKLIST_LIMIT, one can safely assume that the corresponding node is trying to flood the network with possibly fake RREQs. On identifying a sender node as malicious, it will be blacklisted. This will prevent further flooding of the fake RREQs in the network. The blacklisted node is ignored for a period of time given by BLACKLIST TIMEOUT after which it is unblocked. The proposed scheme has the ability to block a node till BLACKLIST_TIMEOUT period on an incremental basis. By blacklisting a malicious node, all neighbors of the malicious Fig.1 AODV routing under (a) Light data traffic load (b) Heavy data traffic node restrict the RREQ flooding.

The neighboring nodes of the malicious node are therefore free to entertain the RREQs from other genuine nodes. In this way genuine nodes are saved from experiencing the Denial of services attack. If the rate of RREQs originated by a node is between the RATE_LIMIT and the BLACKLIST_LIMIT, the RREQ packet is added to a "delay queue" waiting to be processed. Every time a DELAY_TIMEOUT expires, if there is anything in the delay queue (RREQ packet waiting to be processed), then the fIrst packet is removed to be processed. To do so, malicious node that has a high attack rate will thus be severely delayed. Meanwhile, the proposed rate control mechanism will have no impact on other nodes and also have minimal impact on the normal

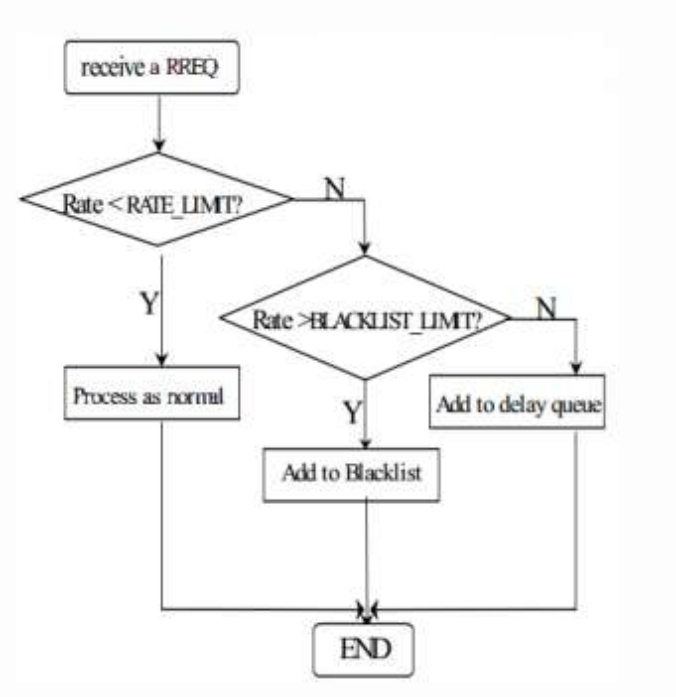
ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

nodes that send abnormally high RREQs. The fIltering forwarding scheme slows down the spread of excessive RREQs originated by a node per unit time and successfully prevents DoS attacks. The proposed scheme incurs no extra overhead, as it makes minimum modifIcations to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV. Also the proposed scheme is more efficient in terms of resource reservations and its computational complexity. In addition to limiting the clogging up of resources in the network, the proposed scheme also isolates the malicious node.

ADVANTAGES

- **Maximize the Network Life Time**
- **Fair Distribution of Energy Consumption**
- **Bandwidth is utilized in efficient way**
- **Multiple topology is accepted**
- **Traffic and congestion is minimized**

SYSTEM ARCHITECHTURE
PERFORMANCE EVALUATION
PACKET DELIVERY RATIO



Ratio of the data packets received at the destination nodes to the packets that were sent by the sources

END TO END DELAY

Includes all the delays encountered by the packet at the different hops from the time it was sent by the source until the time it was received at the destination.

ROUTING LOAD

Number of routing packets (and supporting protocol control packets) transmitted per data packet delivered at the destination.

Channel type	Wireless channel
Radio propagation model	Propagation Two ray ground
Network interface type	Phy/wirelessphy
Mac type	Mac 802_11
Interface queue form	Queue/droptail/priqueue
Link layer type	LL
Antenna model	Antenna/Omni antena
Max.packets in infq.	50
Routing protocol	Hybrid EESM
X dimension topology	1100
Y dimension topology	1100
Model of simulation	Energy model
Initial energy in joules	100
Time of simulation	75.0sec.

SIMULATION PARAMETERS

SYSTEM MODULES

ROUTE MANAGEMENT

- HELLO: Nodes introduce one another using these packets in a network and send them periodically. Absence of hello packets from a node gave the indication about its mobility.
- RREQ: If the source in the network wants to emit the data to destination and no pre-existed route prevails, then the request (RREQ) is broadcasted to the adjacent nodes in the network in a controlled manner. The neighboring nodes further forward the RREQ packets till the destination is found.
- RREP: Then the backward journey of the acknowledgement is initiated in the form of RREP. It is emitted by the nodes that have the direct approach to the destination. The source receives the RREP from various nodes; then it selects the efficient path and starts the awaited transmission after comparing parameters.
- RERR: When the smooth data flow got interrupted and error occurs, the outbreak of RERR packets takes place and the source along with other nodes in the network are made aware of this failure.

QUEUE MANAGEMENT

Passive Queue Management (PQM) algorithm which only sets a maximum length for each queue at the router. Routers decide when to drop packets. It uses first in, first out algorithm. In Drop Tail, the traffic is not differentiated. Each packet has the same priority. When the queue buffer is filled to its maximum capacity, the packets arrived afterward are dropped till the queue is full. That is, Drop Tail will keep discarding/dropping the packet until the queue has enough room for new packets.

Dynamic Queue Size increment –The drop-tail queue has modified in this module. It has fixed queue limit. In modified module The simple drop-tail module drops the packet from the tail when it is overflowing. It transmits (dequeue) the packet in FIFO (First in First Out) manner. In modified module when a packet arrived for buffering, the queue size (byte) is

```
qlimBytes = qlim_ * mean_pktsize_;
```

if occupied queue size with incoming packet size is greater then qlimBytes,the dynamic initialization of queues is performed for the new packet by incrementing queue limited use

```
qlim=qlim+1;
qlimBytes = qlim_ * mean_pktsize_;
q_->length() + 1;
```

In above equation qlim is the instantaneous limit of the queue. mean_pktsize denotes size of the arrived packet.

IV. HYBRID TOPOLOGY MANAGEMENT

1) **Reliable :** Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network.

2) **Scalable:** Its easy to increase the size of network by adding new components, without disturbing existing architecture.

3) **Flexible:** Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.

4) **Effective:** Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high tolerance capability (as each node is not directly connected to other but through central device), so these two can be used effectively in hybrid star-ring topology.

V. CONCLUSION

In our simulations, we conduct the control overhead and the packet delivery rate with random mobility speeds. Simulation results show that the proposed location based EESM-hybrid can reduce the control overhead and increase the route lifetime than AOMDV. Only the forwarding neighboring nodes are involved in routing while the non-forwarding nodes are switched to idle state. This ensures reduction in energy consumption in the network. The results of EESM-hybrid based protocol are very effective as compare to normal AODV routing and energy based AOMDV routing. Routing overhead and packet delivery fraction are shows excellent results with minimum packet loss.

REFERENCES

1. Kavitha, R. Shelgin, S.,, Sandeep, S. "A study on vulnerability detection of attacks in web security",2017,International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No: 9-12
2. Kavitha, R., Priya, N., Anuradha, C., "Li-Fi science transmission of knowledge by way of light",2017, International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:285-290
3. Kavitha, R..,Priya, N., Anuradha, C., "A novel approach of hybrid cloud",2017, International Journal of Pure and Applied Mathematics, Volume 116, 9 Special Issue, Page No:299-304
4. Kavitha, G., Kavitha, R., Koushik Subramaniam, Y. "Operating scheme and its shield in mobilephone by utilizing android",2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue, Page No:129-133
5. Kavitha, R., Kavitha, G."Deconstructing evolutionary programming using ghat",2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:213-216
6. Kavitha, R., Kavitha, G., Thakur, K.A. "Helmet mounted heads-up display a rider assistance smart helmet for everyone",2017,International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page No:411-413
7. Priya, N., Pothumani, S., Kavitha, R,"Merging of e-commerce and e-market-a novel approach",2017,International Journal of Pure and Applied Mathematics,Volume 116,
9 Special Issue ,Page No:313-316
8. Priya, N., Anuradha, C., Kavitha, R" Analysis of various data mining clustering algorithms",2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue,Page No:279-281
9. Kavitha, S., Kavitha, R."DDOS attack and defenses",2017,International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue,Page No: 57-61

10. Kavitha, R., Kavitha, G.,"Decoupling byzantine fault tolerance from multi-processors in I/O automata",2017,International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue,Page No:225-228
11. Kavitha, R., Kavitha, G."A development of IPV4 with skilty approach",2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:219-222
12. Shelgin, S., Kavitha, R."A cram on bluejacking by OBEX (Object exchange)", Volume 2017, International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue, Page No:441-445
13. Shelgin, S., Kavitha, R., Sudha, K.L."Identifying credit card fraud using biometric fingerprint techniques",2017,International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue, Page No: 447-451
14.Kavitha, G., Kavitha, R., Jennifer, S."Effectual exploit of digital irrigate tecniques to afford cloud safety marking",2017,International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue,Page No:185-189
15. Kavitha, R., Kavitha, G., Ramya, B."Inpatient monitoring for healthcare data using wireless sensor network",2017,International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:345-350
16. Kavitha, R. "A methodology for improving read-write technologies for dhts",2017, International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page No:93-97
17. Priya, N., Pothumani, S., Kavitha, R."Analysis of data mining using social network", 2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue, Page No: 307-310
18. Shelgin, S., Kavitha, R."A study on web application security state",2017,International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:75-78
19. Priya, N., Anuradha, C., Kavitha, R."Analysing storage and processing in enhanced cloud computing with hadoop ", 2017, International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue,Page No:293-296
20. Kavitha, G., Kavitha, R.,Indhu.G, "Big Data, Cloud, Web of Thing in Healthcare Monitoring Scheme", 2017, International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page 177-182
21. Kavitha, R., Kavitha, G., "Fuzzy, probabilistic algorithms for online clustering algorithms",2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:207-211
22. Shelgin, S., Kavitha, R., Balasubhakar,"A comparitive study on 5g mobile wireless technology"2017,International Journal of Pure and Applied Mathematics, Volume 116, 9 Special Issue,Page No:81-85