International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Different Solutions to Routing Attacks in MANET

Sunita, T. Pavankumar

Abstract – MANET doesn't need any infrastructure; it is multi-hop network of mobile nodes. Each node can move freely at any direction. We can use wireless devices such as mobile, PDA, tablet, Laptop etc. anywhere at any time. MANET with mobility feature has several challenges, such as dynamic topology, bandwidth constraints and limited battery power etc. Ultra Wide Band MANET has applications in variety of fields such as high bandwidth wireless network for home and offices. UWB can be used in entertainment and emergency services, military communications. UWB MANET nodes are dynamic and every node acts like a router, due to changing topology UWB MANET is vulnerable to malicious attack. Routing attack becomes one of the special problem in UWB MANET several routing protocol AODV, AOMDV, CLSAODV are in existence. All these protocols have limitations one can secure route but not communication data. Proposed protocol will provide both routing and communication security. This work presents a detailed survey on different routing attacks and solutions to these routing attacks.

Keywords- MANET, routing attack, AODV, DSR, DSDV, authentication, non-repudiation.

I. INTRODUCTION

There are large numbers of mobile devices and Mobile ad hoc networks are available [1], [2]. These are used in different applications like special military operations and emergency preparedness. This is all because of their infrastructureless characteristics. Each node in MANET, works as host as well as router. Nodes need coordination while receiving data and forwarding data packets by creating wireless local area network [3]. These characteristics also have some disadvantages if observed for security. Yet some aforementioned applications force some strict constraints on topology. Also on routing and data traffic for security. For example the availability and unity of malignant nodes in the network may interrupt the routing process which fails the network operations. Great research work is done on the security of the MANET. Many of them deal with prevention and detection techniques. The affect of this becomes weak when number of malignant nodes collaborates together to start the cooperative attack. This may lead to more disastrous affects to the network.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
Mrs. Sunita*, Usturge-Nandgave Research Scholar, CSE Department KL University
Dr. T. Pavankumar, Professor CSE Department, KL University

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

If absence of any infrastructure added along with feature of dynamic topology of MANET make such networks endangered to routing attacks like Blackhole and Grayhole attacks (known as forms of blackhole attacks).

In blackhole attacks, malicious information is broadcasted by a node saying that it has the shortest path for destination just to intercept the messages. In such attacks, the malicious so called balckhole node with the help of Forged Route Reply (RREP) attracts all the packets claiming "fake" shortest route is available to reach the destination and then disposes all these packets instead of actually forwarding them to the destination. Whereas in grayhole attack, malicious node cannot be identified at initial stage as it becomes malicious only in later time. This prevents security solutions from finding its presence. And then it selectively forwards or discards the data packets.

This paper focuses on recognizing the grayhole attacks or cooperative blackhole attacks with the help of Dynamic Source Routing (DSR) which uses routing technique. DSR [4] mainly has two main processes:

a) Route discovery
b) Route maintenance

For executing the first phase that is discovery phase, Route Request (RREQ) is broadcasted by source node. If any intermediate node has the destination nodes information in its cache, it replies with RREP to source node. When the Route request is forwarded to a node, the address information is added by node in the RREQ packet. The destination node depends on collected information from the packets for sending the reply message to the source node. DSR has no any kind of detection mechanism but the source node can get all the necessary information of the concerning nodes. In our approach, we have used this feature. In this paper cooperative bait detection scheme (CBDS) is used to detect malicious nodes which tries to attempt grayhole or collaborative blackhole attacks. In our paper, the adjacent nodes address is used as bait destination address. This is used to bait the malicious nodes. The malicious nodes are detected with the help of a technique called reverse tracing technique. The found malicious node is kept separately to the blackhole list so that all the remaining nodes get the alert message to stop the communication to the nodes belonging to that list.

II. RELATED WORK

Many researchers have focused on finding the malicious node in MANET. Many of these solutions work only on detecting single malicious node. This also requires great resources as well as time and cost to identify blackhole attacks. Also, some of these techniques require specific environment [5] or some assumptions in order to operate. Detection mechanisms discussed till date can grouped into two categories:

1) Proactive detection schemes [6] to [12] are schemes that require continuously finding or monitoring neighbor nodes. In such schemes, regardless of the presence of the malicious nodes, the overhead for the detection is continuously created and the resources used for the same are continuously wasted. However it has some advantages like such schemes are helpful in finding such attacks in its early stage.

2) Reactive detection schemes [13] to [15] are started only when destination node finds notable difference in the ratio of delivery of packets

The papers [9] and [13] are considered as benchmarks for differentiation purposes. Liu et al. [9], proposed 2ACK scheme for MANET to detect routing misbehavior. In this scheme two hop packets with acknowledgments are sent back to indicate the successful reception of data packets. But the acknowledgements are delivered in opposite direction. Rack i.e. parameter acknowledgement ratio is used for controlling the acknowledgement requirement. This scheme comes under proactive schemes and thus generates additional overhead ignoring the presence of malicious nodes.

Xue and Nahrestedt in [13] proposed a mechanism for prevention called as BFTR i.e. Best Effort Tolerant Routing. End to end acknowledgement technique is used by this scheme just to observe the routing path's quality preferred by the destination node. That is measured in terms of packet delivery ratio as well as the delay. If the path followed by packets deviates from the predefined one then source node uses new node[14]. The drawback of this scheme is that malicious nodes may still be there in newly chosen route. This actually leads to routing overhead.

The proposed approach considers advantage of the reactive as well as proactive schemes for designing DSR based scheme which finds grayhole or collaborative blackhole attacks in MANET. Personal area networks nowadays are using Ultra Wide Band which is based on ultra wide band technology. This has become very promising in the various applications of MANET & VANET. This is because of their strong capacities like high data rates as well as low power consumption [4]. UWB uses low energy levels [5] and these can be used in short range and high bandwidth (>500MHz). UMB provides long radio range around 150m indoor whereas 1 km for outdoor [16]. This also provides high data rates of 100 Mbps with bit rates of 55,110 and 200 mbps [5]. These are used in Bluetooth technology as it works on low power devices. This is suitable for indoor as well as outdoor applications [14]. UWB has features like proper utilization of bandwidth and maximum range of transmission that is 250m [14], minimum range as 3.12 GHz to 10.6 GHz. The main problem of it is unstable link [8] and its security. MANET has challenges like in channel assignments, its usage, and infrastructure absence also nodes move continuously and the topology keeps on changing. Every node in MANET has capacity to act as a router [2].

Routing in MANET :

Each node in MANET can act as router. This reduces the routing overhead if compared with wired networks. The communication between nodes can only take place if they are in same communication range. If not then they have to communicate through intermediate nodes. MANET nodes don't have any information about topology [12]. The topology should be determined by the nodes. A node tells its presence [7] and obtains information of neighbors. In this way node finds neighbors. Routing is very difficult if have nodes moving continuously. The main objective of routing is to establish the optimal route having minimum overheads and consumes less bandwidth. Destination Sequence Distance Vector (DSDV) and Optimal Link State Routing (OLSR) which come under proactive routing [8] periodically updates the routing tables by sending routing control packets to the neighbor nodes. So are table driven. AODV and DSR are reactive protocols. These protocols send control packets on requirement of route maintenance or route discovery. These are most widely preferred. MANET nodes are more vulnerable to security attacks because of centralized administration, less bandwidth and power consumption and dynamic topology.

Mobile Adhoc Networks and their security is very important aspect if considered the functionality of networks. MANET more often suffers from the security issues because of its features like dynamic topology change as well as cooperative algorithms etc. Various possible attacks are possible on MANETs. It is expected that security of MANETs should be able to handle every type of attack. Security of MANET is different from other networks because of its characteristics like infrastructureless framework etc. Wired networks have specific functionality components like only routers decide the routes of the packets to move from the source to the destination. So security implementation is easy. Whereas wireless networks use infrared or radio frequency signals for communication. These networks can be either infrastructure based or can be infrastructureless. Infrastructure based networks use Public Switched Telephone Network (PSTN) switches and mobile hosts. In ad-hoc networks includes infrastructureless wireless networks perform all networks as routing, packet forwarding and so on. MANETs mainly focus on security of applications related to safety.

Non safety applications require less security. As MANETs are infrastructureless in nature, there is no any prior relationship between the nodes. Nodes can join or leave network anytime without intimating to other nodes.

III. LITERATURE SURVEY

3.1 Routing MANET:

3.1.1 Routing Classification:

For Mobile Ad-Hoc networks, many routing algorithms are proposed. They are classified as:

3.1.1.1 Clustered and Flat Routing:

A. Clustered Routing:

In clustered routing, central controller takes all the decisions. Many of the nodes have hierarchical structure in which nodes are grouped in clusters. Central controller is responsible for the connectivity of the groups and sends the routing information to other member nodes.

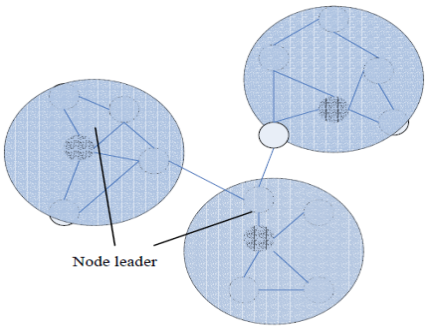

FIGURE 3.1: CLUSTERED ROUTING

Clustered approach may have some disadvantages like delays in broadcasting the information to the nodes. This makes network unfeasible. Movement of nodes causes complexity to the networks [16].

B. Flat Routing:

In Flat routing, the route's computations are shared between the nodes of network. The structure of nodes is distributed unlike in clustering routing. Here all nodes have same work and capabilities. Nodes are responsible for taking their own decisions without being dependent on any central controller. It also does not have any central point of failure. The failed or broken node won't affect the network. These are Destination Sequence Distance Vector (DSDV) [14].

3.2 Classification of MANET Routing Protocols:

Following are the three routing protocols used in MANET:

i) Proactive Protocols
ii) Reactive Protocols
iii) Hybrid Protocols

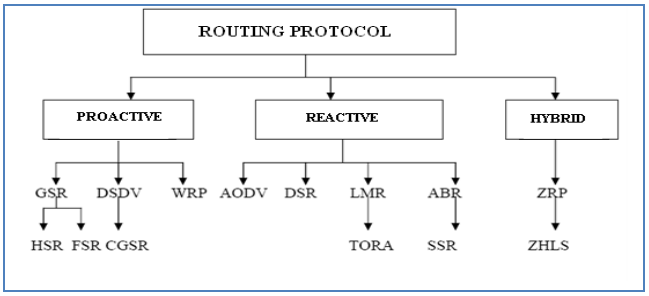

FIGURE 3.2 : CLASSIFICATION OF ROUTING PROTOCOL

- **REACTIVE PROTOCOLS:**

These protocols are also known as Demand Driven Reactive Protocols [8, 9]. The reason why they are called as Reactive protocols is as because they never start the discovery of routes by themselves. Until and unless source node requests for the same. They set up path only when demanded. When any node needs to communicate with another node and source nodes do not have the route then source node communicates with the reactive node. Then these nodes establish the route. The reactive protocols used so far are DSR, AODV and TORA.

Usually Reactive protocols:

- Until demanded, don't find the route
- They use 'On Demand' flooding method to send the query to get the destination information
- They use bandwidth only while transmitting the data to destination node.

AD HOC ON-DEMAND DISTANCE VECTOR (AODV):

Ad Hoc On Demand Distance Vector [9] uses DSR's features like route on demand via same route discovery technique. When route is required, source node broadcasts RREQ packet. Important feature of AODV is sequence numbering. This prevents looping in the network. They are unique and are incremented for every request. The routing table's information will also be updated using these sequence numbers. This has very unique feature like it has only one entry per destination. Multi paths are not supported by this. This has disadvantage when route failure event occurs. When active link fails, AODV has to establish new process which causes additional delay and flooding in network. These algorithms use hello messages those are broadcasted to all neighbors over particular period of time. These messages are nothing but advertisements used for checking the validity of neighbor nodes. If hello message is not received after a specific time span, the neighbor node presumes that node has moved away from the communication range. Failure of link or RRER packet will be circulated to other nodes. RRER informs only to the nodes in route.In this model, RREP is generated by the node either when it itself is destination as well as valid route.

To prevent unwanted RREQs, ring search technique is used. In this technique, node at the begining controls the search using time to live (TTL) field. If RREQ times out, the originator broadcasts it again with greater TTL value. This is continued till TTL gets its threshold value. Though this method minimizes the routing overheads, it generates longer delays. This operates effectively if it is combined with some third party reply methods. The combination of these two would make it easy to find the destination at early stage.

Dynamic Source Routing (DSR):

This belongs to the reactive routing [5][13]. This allows nodes to dynamically find the route to the destination. In this technique, packets follow the hop by hop route to destination. This uses route discovery technique to determine the unknown destination route dynamically. If you want to send some packets to the destination that is unknown, the source node floods the network with RREQ. When the destination is found, RREP i.e. Route Reply will be sent back to the source node by following the same track. This acts only on demand. No periodic updates are used here. No mechanism is used for removing stale routes. The route will be used by network till it is valid or available.

- **PROACTIVE PROTOCOLS:**

Proactive protocols [6] work differently if compared with the Reactive protocols. The protocols constantly check the updated topology. Every node in the network knows every other node of the network. Complete network is known to all the nodes of the network. The routing information is separately maintained in different tables. When network topology is changed, tables are updated. The nodes also share the network topology and change information with each other. Also get the information of route whenever required. The Proactive protocols are DSDV and OLSR.

DSDV (Destination-Sequenced Distance-Vector Routing):

Destination Sequenced Distance vector Routing is table driven routing scheme for Adhoc Mobile Networks. This is based on Bellman. This is not so efficient because as the network grows the overhead also increases [10]. This is mainly designed for solving the routing problem. The routing table maintains the sequence number. The even sequence number indicates the presence of link where as odd number indicates the absence of link. This requires timely updating the routing table. This uses battery power and some bandwidth even though network is in idle state.

HYBRID PROTOCOLS:

These protocols use the strengths of reactive as well as proactive protocols and combine these features to get more refined results. The network is partitioned into different zones and different protocols are used for two zones. The example of Hybrid Routing Protocol [6,17,18] is Zone Routing Protocol. ZRP uses proactive mechanism to establish the route and uses reactive protocols for communication. Local neighbors are called as Zones so the protocol is named as Zone Routing Protocol. The zone's size is represented by radius p. Where p is the number of hops.

IV. ROUTING ATTACK IN UWB MANET & VANET

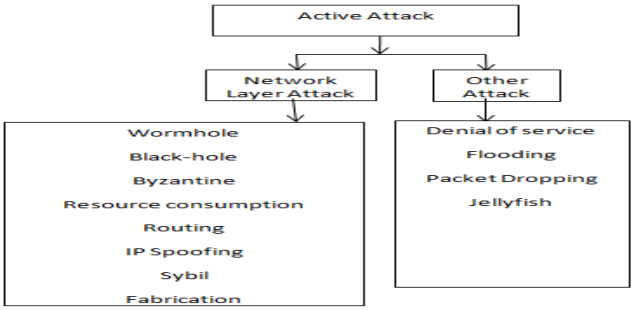

Figure 4.1: Routing attacks in UWB MANET

Routing Attacks mainly classified as passive and active attack.

Passive attacks without disturbing the routine operations of the network, try to obtain the information so they are very difficult to identify.

Example: Traffic analysis, traffic monitoring, and eavesdropping Traffic analyzing attacker attempts to find the path from sender to receiver [13].Traffic monitoring attacker can read confidential data but cannot edit packet data. MANET eaves dropping attacker finds the secret data such as private key or public key of anyone either senders or receivers.

Active Attacks can interrupt network operation by either changing or deleting information or by inserting a wrong message or impersonating a node.

Example: Modification of messages, impressing the nodes, fabrication or jamming message replay. Fabrication attack, where a malicious node generates false or incorrect information. Jamming attack occurs at physical layer.Message replay attack is one in which malicious node duplicates data or delayes data. Even it intercept password as well.This paper mainly focuses on routing attacks.

Routing attacks:

A. Wormhole attack:

In wormhole attack malicious node connect two disjoint points in space, here also by short-circuiting the network MANET one or nodes routing can be interrupted.

Solution to wormhole attack:

i) Geographical leashes & temporal leashes

To restrict the distance of packet, a leash is added. Leash is associated with every hop. For transmission of packets, new leash is required. The geographical leash is responsible for maintaining the transmitter and receiver distance. Temporal leash is used as an upper bound as lifetime for packets.

ii)Using directional antenna

Restrict deviation of signal propagation through air to avoid packet dispersion.

B. Blackhole attack:

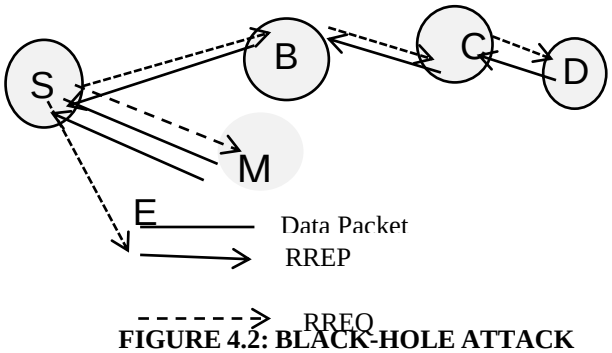

FIGURE 4.2: BLACK-HOLE ATTACK

In black-hole attack malicious nodes act like a black-hole which discards all data packets passing through.

Solution to black-hole attack:

Maintain a table [15] at every node along with the previous sequence number in ascending order. Before forwarding the packets, every node increments the sequence number. RREQ and RREP plays important role here. If RREP obtains incorrect sequence number, it comes to know that something has gone wrong.

C. Byzantine attack:

Intermediate nodes set tasks between sender and receiver which perform changes like routing loops creation, sending packets through non-optimal path for selectively dropping packet which disrupt routing services.

D. Spoofing

Malicious node wrongly gives its identity so sender will change the topology.

E. Sybil attack:

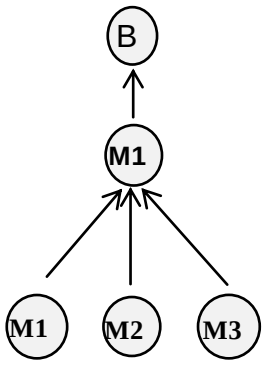

Figure 4.3: Sybil Attack

In Sybil attack, the malicious node shows itself by creating many fake identities and by pretending to have multiple nodes in the network. One single node assumes a role of multiple nodes and can monitor or affect multiple nodes at a time.

Solution to Sybil attack:

By maintaining chain of trust. This generates single identity for hierarchical structure.

F.DOS attack:

Denial of Service (DOS) attack, malicious node consumes bandwidth of the network. When a message arrives from unauthenticated node, the receiver does not receive that message because the receiver is busy and hence beginners have to wait for the receivers reply.

G. Flooding attack:

In this attack the attacker node floods the complete network with some very high quality routes and the powerful transmitters.

H. Jellyfish attack:

Attacker node changes the sequence of some of the packets before forwarding them.

Solution to Jellyfish attack:

2ACK, where S sends data packet to D, Destination reverts back a special two hops acknowledge indicating data received.

V. THE PROPOSED METHODOLOGIES

Nidhi Lal [1] proposed method to find malicious node behavior via I-watchdog protocol in MANET with DSDV routing scheme.

Watchdog Protocol: This protocol is a process of sending data from one node to next node, if the sending time of the subsequent hop neighbor node is superior to the packet storing time and go beyond specific predefined threshold of the network at that time Watchdog discern that system is under black-hole attack, and it instantly detects as a malicious node [16].

Disadvantage of watchdog: It does not sustain mobility with large number of nodes and causes packet loss.

Disadvantage of I-watchdog: Improved-Watchdog protect a network from black-hole attack which leads to denial of service attack.

SUPERMAN Methodology

Authentication of Node, network access control and secure communication are provided in MANET [3].

Advantage

It can guarantee secure routing as well as communication security.

Drawback

Mainly focus is on network layer, rather than data link and physical layer.

DCFP Methodology

Dynamic Connectivity Factor (DCFP) has been developed, where DCFP refer neighbour based dynamic connectivity factor [4].

It uses connectivity metric to provide accurate information about the nodes.

Advantage

DCFP can reduce RREQ overhead with the help of a new connectivity factor

Drawback
Protocol doesn't work for varying node speed.

NCPR Methodology
A probabilistic rebroadcast protocol (NCPR) [5] considers neighbor coverage to minimize the routing overhead in MANET.

Advantage
The rebroadcast delay is calculated by NCPR dynamically which is used for the forwarding order and utilize neighbour coverage knowledge.

Trust Prediction Methodology
There are different trust prediction approaches one is neighbor sensing (direct trust) and other is recommendation based (Indirect trust) and third approach is hybrid method [6].

Advantage
Trust propagation, aggregation, and predictions are analyzed.

Drawback
Trustworthiness model proposed is vulnerable to collusion attack.

HBDADCS Methodology
Proposed solution detects black-hole attack namely honeypot based dynamic anomaly detection (HBDADCS) [7].
The effectiveness of the proposed technique depends on the cross layer security.

Advantage
The honeypot approach detects and isolates black hole attack from the network.

Drawback
Only two layers MAC and routing considered with minimum features.

Trust based certificate revocation Methodology
Proposed CA distribution and a Trust based threshold revocation method [8].

Advantage
This method provides security for multipath routing protocol as well as for data transmission with multipath route.

Drawback
This work has not developed extensive models for security attacks, and a reliable security framework against all possible security attacks in an ad hoc network.

Security using Hash Methodology
Zone Routing Protocol (ZRP) and hashing algorithm, keyed-Hash Message Authentication Code – Secure Hashing Algorithm [10] for the Authentication and Data Integrity of the information are used.

Advantage
HMAC SHA 512 provides data integrity and authentication

Drawback
This method increases end to end delay.

Control packets Methodology
Proposed method is used to avert the malicious node and discover the secured routes in the MANET [12].

Advantage
At the initial stage itself the malicious nodes are identified and removed quickly so that it cannot take part in further process.

Drawback
Packet delivery ratio (PDR) is increased with negligible difference in routing overhead.

VI. CONCLUSION

According to the above work, it can be concluded that performance of UWB MANET can be increased. The main focus of the proposed paper is for securing multiple routing protocols and also data transmission with multiple routes.The work is looking forward to use Modified Ad-hoc on demand Distance Vector (MAODV) protocol. MAODV is the best suitable for UWB MANET & VANET. For secure transmission various approaches can be used such as message digest, certificate, etc. Digital signature based routing performs excellent but they are well suited for highly dense networks.

Table I: Comparisons of routing protocols

Protocol/ Parameter	QOS Metric	Bandwidth Estimation	Route Discovery	Resource Reservation	Route break prediction	Authentication
OLSR	BW	NO	Proactive	NO	NO	NO
EMAODV	BW, Delay	YES	Reactive	YES	NO	NO
CLSAODV	BW	NO	Reactive	YES	YES	NO
SAODV	BW	NO	Reactive	YES	YES	NO
ALARM	BW	YES	Proactive	YES	NO	YES
I-Watchdog	BW	YES	Reactive	YES	NO	YES

REFERENCES

1. SUPERMAN: security using pre-existing routing for mobile ad-hoc networks IEEE Transaction on Mobile Computing 2016.
2. Ali Mohamed E. Ejmaa1, (Member, IEEE), " Neighbor-Based Dynamic
3. Connectivity Factor Routing Protocol for Mobile Ad Hoc Network," IEEE Access 10, Vol No. 4, pp. 8053-8064, June 2016.
4. Nidhi Lal, "Detection of malicious node behavior via I-Wathdog protocol in MANETwith DSDV routing scheme", Science Direct, Procedia Computer Science 49 (2015) 264 – 273.
5. Banoth Rajkumar, Dr. G. Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET & VANET",2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), pp. 431-444, April 2016.
6. Arathy K S, S Minesh C N, "A Novel approach for detection of single and collaborative Black hole Attacks in MANET & VANET", Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology(RAEREST2016) Science Direct.

7. Pawan Kumar Sharma, Vishnu Sharma, "SURVEY ON SECURITY ISSUES IN MANET Wormhole Detection and Prevention", International Conference on Computing, Communication and Automation (ICCCA2016), ISBN: 978-1-5090-1666-2/16/$31.00 .
8. Anuj Ranaa, Vinay Ranab, Sandeep Gupta, "EMAODV: Technique to Prevent Collaborative Attacks in MANET & VANET", 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015, October 2015.
9. Mr. Suketu D Nayak and Prof. Sunil J. Soni, "Securing AODV for MANET using Message Digest with Secret Key", January 2011, https://www.researchgate.net/publication/261437510.
10. Todd R. Andel, Alec Yasinsac, "Link Stability and Energy Aware Routing Protocol in Distributed Wireless Networks", IEEE transactions on parallel and distributed system, vol. 23, NO. 4, April 2012.
11. Arvind Dhaka, "Gray and Black Hole Attack Identification using Control Packets in MANET", Elsevier, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015) Feburary 2015.
12. Charles E. Perkins and Elizabeth M. Royer, "KNN Query processing methods in MANET & VANET", IEEE TRANSACTIONS ON MOBILE COMPUTING, Vol. No. 13, No. 5, May 2014.
13. Anirudhha Bhattacharya, "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques", Department of science and Engineering Institute of Engineering, Saltlake, http://www.doc88.com/p-410724870368.html.
14. Atul B.Kathole , Yogadhar Pande "Survey Of Topology Based Reactive Routing Protocols In VANET" International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 39 ISSN 2229-5518.
15. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 2, February 2012) 6 Detection of Misbehaving Nodes in Ad Hoc Routing Isha V. Hatware , Atul B. Kathole , Mahesh D. Bompilwar
16. Rutuji Jahavri, "DOS Attacks in Mobile Ad-hoc Networks", 2nd International conference on Advanced Computing & Communication Technologies, 2012 IEEE.
17. "Performance Evaluation of AODV with Blackhole Attack", International conference Methods and Models in Science and Technology, 2010.
18. Li-Na Weng, Jie Yang "A cross-layer stability-based routing mechanism for ultra wideband networks", Computer Communications 33 (2010) 2185–2194
19. Mike Burmester, Member, IEEE, Breno de Medeiros Member, IEEE, "On the Security of Route Discovery in MANET", IEEE TRANSACTIONS ON MOBILE COMPUTING, Manuscript received April 26, 2007; revised March 1, 2008.
20. Djamel DJENOURI, Nadjib BADACHE, "A survey on Security issues in Mobile Ad hoc Networks", February 2004, Laboratories des, systems informatiques.
21. Ajay Jadhav and Eric E. Johnson, Senior Member, IEEE, "Secure Neighborhood Routing Protocol", paper 941.