ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

A Review on Network Layer Security in Wireless Sensor Network

ShaziaSulthana[1], Sindhu Shree[2]
Assistant Professor[1], M.Tech Student[2]
Department of ECE
Global Academy of Technology, India

Abstract:
As the Wireless Sensor Networks (WSN) prove to be more beneficial in real-world applications. The Wireless Sensor Networks are no less vulnerable. The attacks on WSN prove to be even more destructive than those on internet or other ad hoc networks. Resource limitations of WSN make these threats even more dangerous, even up to the extent of the consumption of a whole node or even a complete small network. The foremost concerned security issue in WSN is to protect the network layer from malicious attacks, thereby identifying and preventing malicious nodes. A unified security solution is in very much need for such networks to protect both route and data forwarding operations in the network layer. Without any appropriate security solution, the malicious nodes in the network can readily act to function as routers. In this paper a study that will through light on attacks and protections in network layer is presented.

Keywords: Wireless Sensor Network, Network layer attack

I. INTRODUCTION

The advances on miniature techniques and wireless communications have made possible the creation and subsequent development of Wireless Sensor Networks (WSN) paradigm. The main purpose of WSN is to serve as an interface to real world, providing physical information such as temperature, light, radiation etc. to a computer system. The major difference between this type of networks and wired networks is their decentralized and specialized nature. In WSN all its members collaborate towards the common goal of obtaining or deducing certain physical information from their environment.

Moreover WSN is capable of self-organization, thus it can be deployed in a certain context without requiring the existence of a supporting infrastructure. As in all the computing environments, it is essential to assure the proper functionality of WSN in order to allow the correct provisioning of services. Such network should comply with certain security requirements, such as confidentiality, integrity, authentication and others derived from application context. However achieving this goal is not an easy task for WSN.

The reason is the WSN consists of nodes with very limited resources whereas the attacker may have very powerful attacking (malicious) resources such as laptops with wireless LAN capability, long range wireless communication capability etc. Therefore security in WSN is a major issue. The security techniques of the normal computer networks cannot be implemented in WSN because of limited resources. Considering, for example, the asymmetric cryptographic algorithm (such as RSA with 1024 bits) the memory of a typical sensor node is not sufficient enough to hold even the variables for its implementation. Even if memory is allowed the computation time would be enormous.

To worsen the situation the power available with a sensor node is also very small (and the node may entirely consume even in a single computation). So we may conclude that the normal computationally heavy algorithms of security can't be applied on the *weak (*resource limited) *WSN*. The paper is organized as follows. Section 2 describes the operation of Wireless Sensor Networks. Section 3 describes the security classes. Section 4 explores various types of threats and attacks against wireless sensor network with probable countermeasures. Finally Section 5 concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

II. OPERATION OF WSN

A WSN is a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing, to fulfil different application objectives. The major elements of WSN are the sensor nodes and the base stations. In fact, they can be abstracted as the "sensing cells" and the "brain" of the network, respectively.

Usually, sensor nodes are deployed in a designated area by an authority and then automatically form a network through wireless communications. Sensor nodes are static most of the time, whereas mobile nodes can be deployed according to application requirements. One or several, static or mobile base stations (BSs) are deployed together with the network. Sensor nodes keep monitoring the network area after being deployed. After an event of interest occurs, one of the surrounding sensor nodes can detect it, generate a report, and transmit the report to a BS through multi-hop wireless links.

Collaboration can be carried out if multiple surrounding nodes detect the same event. In this case, one of them generates a final report after collaborating with other nodes. The BS can process the report and then forward it through either high quality wireless or wired links to the external world for further processing .The WSN authority can send commands or queries to a BS, which spreads those commands or queries into the network. Hence, a BS acts as a gateway between the WSN and the external world. An example is shown in Figure 1.

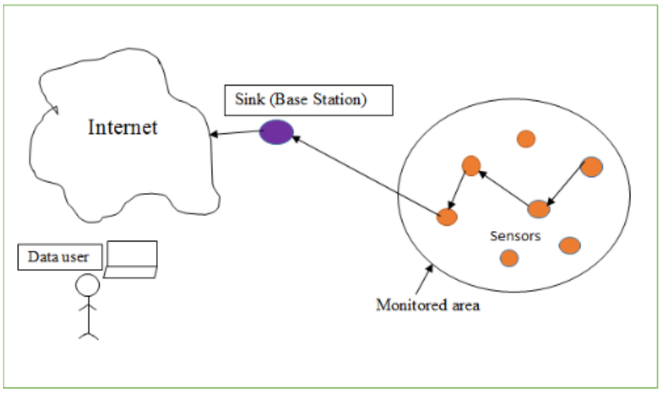

Figure.1.Wireless Sensor Network

III. SECURITY CLASSES

Attacks on wireless network can be broadly classified as interception, modification and fabrication.

- Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain un-authorised access to sensor nodes or data within it.
- Modification is an attack on integrity. Modification means an un-authorised party not only accesses the data but tampers it, for example by modifying the data packets being transmitted.
- Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed.

IV.ATTACKS IN NETWORK LAYER

A. BLACK HOLE ATTACK

In black hole attack, the attacker makes use of vulnerabilities in routing discovery method of AODV, DSR routing protocols [4]. When a source node needs to send data to destination node it broadcast RREQ request to all. So that the node with highest destination sequence number than the current destination sequence number of node will reply and the destination sequence number is higher than current destination sequence number. Then they send this to the source node. Receiving this false RREP packet the source node will select the path through this malicious node assuming that it is the fresh shortest path towards destination. The source node then rejects the RREP packet from other nodes and start sending packet through malicious node. Then this malicious node can drop the packet instead forwarding it. This type of attack is called black hole attack [1].

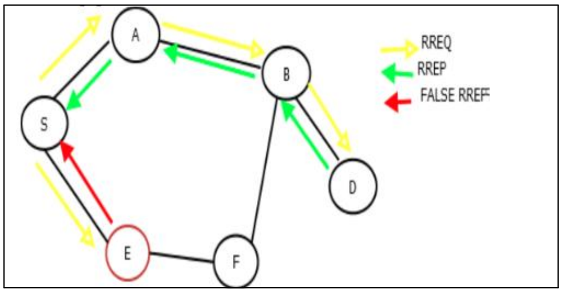

Figure.2. Black Hole Attack

In this example when a data packet is need to be sending from source node “S” to destination node “D” it sends RREQ packet to the neighbors. When node “E”, that is the malicious node receives the RREQ request it sends RREP packet advertising itself having shortest route to destination and it rejects the RREP packet from the legitimate route <S,A,B,D>.The source node S starts sending the packet through <S,E,F,B,D> route and node E that is the black hole attacker can drop the packet passing through them.

B.PROTECTION AGAINST BLACK HOLE ATTACK

Mainly three mechanisms are used to defend against black hole attack. They are TOGBAD, SAR protocol and DPRAODV protocol.

1.) TOGBAD: TOGBAD is a black hole detection mechanism based on topology graph. It compares the number of neighbors a node should have and actual number of neighbors a node have in accordance with the graph. TOGBAD protocol have a drawback that it is possible only for pro-active routing protocol- OLSR where we can obtain topology information but obtaining complete topology information for reactive routing protocol will not be feasible.[4]

2.) SAR (Secure aware routing protocol):The secure aware routing protocol is based on on-demand protocol like AODV or DSR. In original protocol if a node want to send information to other node it broadcasts a Route request packet to its neighbors and they get RREP packet in return indicating the shortest path to destination. In most of the routing protocol they mainly aim at discovering the shortest path from source to destination that is they are considering only the length of the route. But in SAR it incorporates a security metric into the RREQ packet, so that the change of forwarding action depends on RREQs. Whenever a RREQ packet is received by an intermediate node the SAR ensures that the node can process that packet or forward it only if that intermediate node provides required authorization. The RREQ packet is dropped if the node cannot provide the required security. The main drawback of SAR protocol is that we cannot guarantee that the route discovered by SAR between source and destination is the shortest route. But it finds route which guarantee security.SAR is not able to find shortest route because all the nodes in the shortest route may not satisfy the security requirements. If all the nodes in shortest route satisfy the security requirements then SAR can find the shortest route.[13]

***3.)* DPRAODV (Detection, Prevention and Reactive AODV):** In DPRAODV protocol it uses a dynamically updating threshold value .In normal routing protocol like AODV the RREP packet is accepted only if they have a destination sequence number higher than one in the routing table. But in DPRAODV it uses a threshold value. Here it checks whether the destination sequence number of RREP is higher than the threshold value or not .If it is higher than threshold value then the node is said to be malicious node and this node is added to a blacklist .Then the neighbors of this node are alerted by sending a control packet called ALARM packet. These ALARM packets parameters are blacklisted nodes. So if node receives packet from the blacklisted node they simply discard the RREP packet. It also blocks the repeated reply from the malicious node there by reducing the network traffic and thus DPRAODV isolates the malicious node from the network.[16]

C. WORM HOLE ATTACK

In wormhole attack, two malicious nodes make a tunnel between them. This tunnel between them is called wormhole .Here the data packets are attracted to it by advertising itself having shortest path to destination. When a wormhole attack happens in a network it prevents the discovery of other routes than route through wormhole. Thus all the data will be passing through wormhole only. So it can drop the packets as well as can listen to confidential information or can alter the transferred data packets.

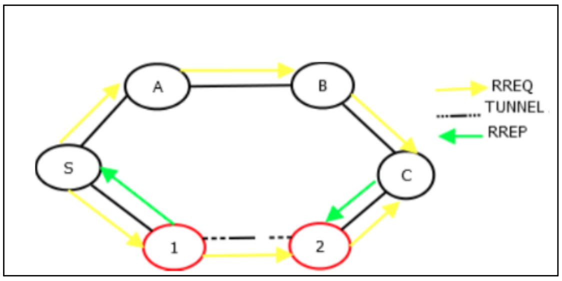

Figure.3. Wormhole attack

In figure3, the nodes “1” and “2” are malicious node and they together form the tunnel in network. The source node “S” sends the RREQ message to immediate neighbours to find the route. The immediate neighbours of source node “S” are “A” and “1”. When node 1 receives the RREQ request it immediately shares with node 2 and then sends RREQ message to its immediate neighbour C that is the destination. As the link between 1 and 2 having high speed the source node selects the route <S,1,2,C> for destination. It results in “D” to ignore RREQ that arrives from legitimate route <S,A,B,C>.

D.PROTECTION AGAINST WORMHOLE ATTACK

The wormhole attack can be defended in two ways they are Packet leashes and sector.

1) ***PACKET LEASHES:*** One of the mechanisms used for wormhole detection is called packet leashes. Mainly leashes means packet that restrict the maximum allowed transmission distance of a packet. There are two types of leashes they are geographical leashes and temporal leashes.

A .Geographical leashes**:** This type of leashes makes sure that that the recipient of the packet is within a certain distance from the sender. To create a geographical leash, each node should know its own location and all nodes clock should be synchronized loosely. The mechanism in geographical leashes is that when a sending node sends a packet it includes two parameters within it. They are location of sending node (ps) and the time at which it sends the packet(ts).When a receiving node receives this packet they compares these values to its own location(pr) and time at which it receives the packet(tr). If senders and receivers clock are synchronized within $\pm\Delta$, and v is an upper bound on the velocity of any node then the receiver can compute an upper bound on the distance between the sender and itself, say *dsr*. Using the parameters timestamp *ts*in the packet, the local receive time *tr*, the maximum relative error in location information , the locations of the receiver *pr*and the sender *ps*, the *dsr* can be bounded by $dsr \_ ||ps - pr|| + 2v \cdot (tr - ts + \Delta)$ +sigma for authentication of location by receiver. We can use authentication techniques like RSA for this. The main disadvantage of geographical leashes is that if any obstacle comes in communication between two nodes that would otherwise in transmission range then bounding of distance between sender and receiver method fails.[10]

b. Temporal leashes: This type of leashes make sure that packet have a particular lifetime, that allows packet to travel only at a certain distance .In temporal leashes the sender sending the packet will contain a packet expiration time that doesn’t allow the packet to travel further than a particular distance say L. Consider that the maximum synchronization error is Δ and value of this should be known by all the nodes in the network .Thus L>Lmin =Δ.C where c is the propagation speed of our wireless signal. Let the local time at which sender sends the packet is ts so the expiration time is set as te = ts + L/c –Δ .When the receiver get this packet at local time tr it checks whether the expiration time is exceeded or not that is it check that tr greater than te or not. If this is true the receiver will drop the packets. Here TIK protocol is used for authentication of broadcast communication [10]. The main disadvantage of temporal leashes is that within restricted time the packet should be passed through the wormhole [15].

2) ***SECTOR (Secure tracking of node):*** In this method the wormhole attack is prevented by bounding the maximum distance between two neighboring nodes by a series of first one bit exchange. This uses a special hardware to make sure the accuracy of time as well fast processing between the sender and receiver [8].

E. GRAYHOLE ATTACK

Gray hole attack is special variation of black hole attack. In black hole attack the attacker places itself in between the source. The attacker attracts the data packets to it by advertising itself having the shortest route to destination and then they capture the data packet and drops it. In gray hole attack the data packets are dropped selectively or in statistical manner. For instance they may drop packets from a particular node or in some other pattern[4]

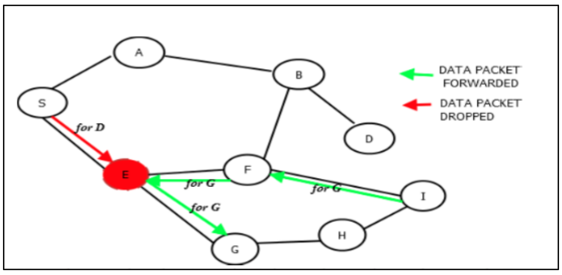

Figure.4. Gray hole Attack

Here the attacker that is node E drops the packet only to node D and it forwards packet from other nodes creating a gray hole.

F.PROTECTION AGAINST GRAYHOLE ATTACK

In a gray hole detection mechanism each node have to generate all evidence on forwarding packets by making use of a aggregated signature algorithm. This algorithm detects whether packets have dropped or not and thus finds the malicious node. Another mechanism used in the gray hole attack is that all nodes maintain their neighbours data forwarding information .After a time interval each node checks if any neighbour with whom it has not communicated and then it starts the detection procedure for the node. This detection is done by comparing the number of RTS and CTS messages. If they found the node to be suspicious then it enquires its neighbours and after that they take decision about the suspected node[4].

G. RUSHING ATTACK

One of the property of an on-demand routing protocol is that nodes are only allowed to forward the first RREQ that arrives for routing discovery and it discards all other RREQ that come late. This property is exploited by rushing attack. The attacker will transmit the RREQ request earlier and thus it suppresses the legitimate RREQ. In most powerful rushing attack they use a wormhole to rush packets.

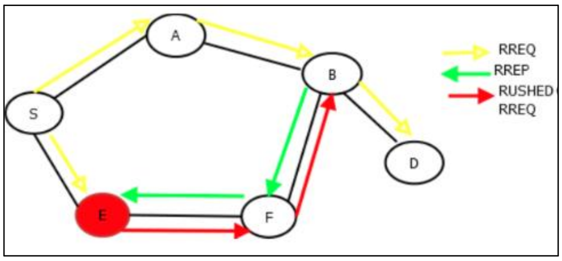

Figure.5. Rushing attack

For example, in figure the node “E” represents the rushing attack node, where “S” and “D” refers to source and destination nodes. The rushing attack of compromised node “E” quickly broadcasts the route request messages to ensure that the RREQ message from itself arrives earlier than those from other nodes. This result in when “C” i.e. neighbouring node of “D” when get the legitimate route request from source, they simply ignore the request. So in the presence of such attacks “S” fails to discover any useable route or safe route without the involvement of attacker.

H.PROTECTION AGAINST RUSHING ATTACK

To prevent the rushing attack we can use three mechanisms together they are secure neighbour detection, secure route delegation and randomized route request forwarding. In on demand protocol if node2 receives broadcast message from node1 then node2 consider node1 as neighbour. If we finds that node1 is neighbour to node2.It gives a route delegation message to allow node2 to forward the route request. If node2 finds that node1 is within range then it gives a accept delegation message. The randomized selection of the route request message to forward make sure that selected path is a low latency path through which requests are forwarded. In secure neighbour detection, each neighbour are allowed to verify that the other node is within a given maximum transmission range. Here we use a three round mutual authentication protocol that uses tight delay timing that make sure that the other node is within the transmission range. In the first round the starting node sends a neighbor solicitation packet by unicast method or broadcast method. In next round by receiving the neighbour solicitation packet the received node sends back a neighbour reply packet. At final round the starting node sends neighbour verification packet containing broadcast authentication of a timestamp and source to destination link. Source route delegation mechanism is used to verify that all the secure neighbour detection procedure are performed between two neighbouring nodes. To explain the mechanism let us consider two neighbouring node n1 and n2,here n1 gets a route request from node S with sequence id, that is destined to node R. Node n1 does the neighbouring detection protocol and find that n2 is the neighbouring node that is within range and then it delegates the route request to n2.The delegation of route request to n2 is given as follows:

MA = (ROUTE DELEGATION; *A*; *B*; *S*; *R*; *id*)
_*MA* = Sign (*H* (*MA*))
A->B: (_*MA)*

Here node n2 can rebuilt the message fields and verify the signature. The node n2 will accept the route delegation if n2 find n1 within the range and this procedure is done to next neighbours and so on. The route delegation message can be incorporated with the last message of secure neighbour detection protocol. In randomized message forwarding random selection technique can be used to prevent the rushing attackers in dominating all other routes to destination. Two parameters are used for selection of randomized forwarding they are the number of request packets to be collected and algorithm which can choose timeouts. If the number of requests chosen is very large, the randomized forwarding will rely more on the time out, which increase the latency and reduce the security. If we can know the complete topology information the timeout must be based on the number of legitimate hope between the starting node and node forwarding the request. But when topology information is not available then node can choose the timeouts randomly [9].

I. SYBIL ATTACK

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. That is the attacker can either use random identity or the identity of legitimate node. This type of attack is called Sybil attack. These attack cause lot of packets to be routed towards the fake identity nodes which makes severe attacks. The presence of this type of attack makes it difficult to find misbehaving node, and also this prevent a fair resource allocation among the nodes [1].In figure 6 it is shown two types of nodes one is trusted group of nodes and other is Sybil attacker nodes .The Sybil attackers are basically nodes with random identity or identity of a legitimate node. The link from the trusted node region to Sybil attacker region helps the Sybil attacker to capture information send through it.

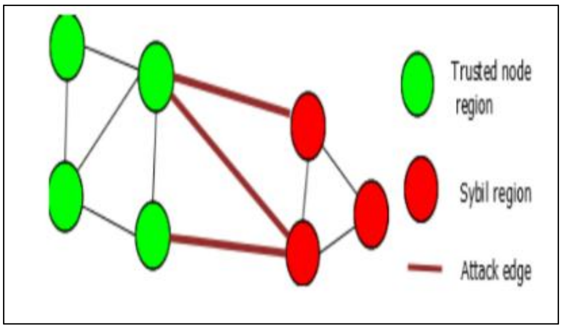

Figure.6. Sybil Attack

J.PROTECTION AGAINST SYBIL ATTACK

There are mainly two methods to detect the Sybil attack they are PASID (Passive ad-hoc Sybil identity detection) and PASSIVE-GD. In passive ad-hoc Sybil identity detection a single node can detect Sybil attacker by recording the identities like MAC or IP addresses of other nodes that hears transmission. By this addresses the node builds a profile of which nodes are heard together. Thus this method helps in revealing the Sybil attackers. When the network contains more nodes in less space the rate of false positives will increase. Thus the node will have only fewer chances to hear its neighbours. To prevent this we have a method where multiple trusted nodes can share their observation with other nodes to increase the accuracy of detection. Next method used for detection of Sybil attack is PASIDGD that is mainly an extension of PASID. This method is used to reduce false positives that may occur when a group of nodes moving together is identified as a single Sybil attacker. Here they exploit the property of channel, that is a single channel transmits only serially and independent nodes transmit in parallel that makes considerably higher collision. So by detecting collision at MAC level we can identify the Sybil attacker of this type [7].

V.CONCLUSION AND FUTURE WORK

Providing security in a wireless sensorq network is a challenging task. In this paper a survey of various threats expected at network layer and their possible protection mechanism of the sensor networks. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. In future there may be ways to defeat these protection mechanisms. So this is a further potential area of research that more powerful detection mechanisms can be invented.

VI. REFERENCES

[1]. Gangandeep, Aashima, Pawankumar "Analysis Of Different Security Attacks In MANETs On Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[2]. Mangesh M Ghonge,Pradeep M Jawandhiya,Dr M S Ali "Countermeasures Of Network Layer Attacks In MANETs" IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[3]. G S Mamatha, Dr.S.C.Sharma "Network Layer Attacks And Defense Mechanisms In MANETS-A Survery" International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010.

[4]. Adnan Nadeem ,Michael p Howarth ,"A Survey of MANET Instrusion Detection & Prevention Approaches for Network Layer Attacks",Proc. IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013.

[5]. Isha V Hatware,Athul B Kathole,Mahesh D Bompilwar "Detection of Misbehaving Nodes in Ad Hoc Routing" International Journal of Emerging Technology and Advanced Engineering (ISSN 22502459,Volume 2,Issue 2,February 2012).

[6]. JyotiThalor, Ms. Monika," Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review" International Journal of Advanced Research in Computer Science and Software Engineering (ISSN: 2277 128X Volume 3, Issue 2, February 2013).

[7]. ChrisPiro, Clay Shields, Brian Neil Levine "Detecting the Sybil Attack in Mobile Ad hoc Networks".

[8]. Xia Wang, Johnny Wong "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks"2007 31st Annual International Computer Software and Applications Conference (ISBN: 0-76952870-8).

[9]. Yih-Chun Hu, Adrian Perrig, David B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols",Proc.2nd ACM workshop on Wireless security Pages 30 - 40 .

[10]. Yih-Chun Hu, Adrian Perrig, David B. Johnson "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks"Proc. INFOCOM 2003. Twenty-Second Annual Joint Conferences of the IEEE Computer and Communications. 2003 , Page(s): 1976 - 1986 vol.3 .

[11]. Diogo Miguel da Costa e Castro M´onica Oliveira "Thwarting the Sybil Attack in Wireless Ad Hoc Networks".

[12]. Tran Van Phuong, Ngo TrongCanh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee "Transmission Time-based Mechanism to Detect Wormhole Attacks".Proc.2nd IEEE Asia-Pacific Service Computing Conference (APSCC 2007), ISBN: 0-7695-3051-6.

[13]. Seung Yi, Prasad Naldurg, Robin Kravets "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks" Proc. MobiHoc '01 Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing Pages 299-302.

[14]. Brian Neil Levine, Clay Shields, N. Boris Margolin "A Survey of Solutions to the Sybil Attack",Tech report 2006-052,University of Massachusetts Amherst, Amherst, MA, October 2006.

[15]. Jackson Kwok "A Wireless Protocol to Prevent Wormhole Attacks"proc. A Thesis in TCC 402 March 23, 2004.

[16]. Ketan S. Chavda , Ashish V.Nimavat "Comparative Analysis Of Detection and Prevention techniques of black hole attack In aodv Routing protocol of MANET " International Journal of Futuristic Science Engineering and Technology, Vol 1 Issue 1 January 2013 ISSN 2320 – 4486.

[17]. Amit M Holkar, Neha ShindeHolkar and Dhiiraj Nitnawwre " Investigative analysis of repudiation attack on MANET with different routing protocols" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 3, May – June 2013 ISSN 2278-6856 .