DDBA-DSR: Detection of Deep Black Hole Attack in DSR

[1]Mamta
Student
Deenbandhu Chhotu Ram University Of Science & Technology, Murthal, Sonepat(Haryana), India

[2]Suman Deswal
Assistant Professor
Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonepat (Haryana), India

ABSTRACT

A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructure less, multi-hop network and mobile nodes are free to move in any network. Due to their lack of centralized control, and dynamic topology, MANETs are vulnerable to many attacks. From a security design perspective, there is no built-in security. So, security is one of the main concerns in ad hoc networks. In this paper, a technique DDBA-DSR is presented to protect against the deep black hole attack. Deep black hole is an extended black hole attack that advertises fake RREQ in response to received RREQ as well as overheard RREPs. In this present work, a hybrid mechanism is presented that will perform the detection as well as the prevention to these kind of attacks. Our work is performed in two phases: first, setting criteria for such nodes and secondly, to perform communication along a safer path.NS2 is used for simulation and evaluation of the network parameters.

Keywords

MANET, DSR, routing protocol, deep black hole attack.

1. INTRODUCTION

MANET (mobile ad hoc networks), a wireless network, is an autonomous collection of the mobile nodes that are dynamically connected in the network. MANETs are infrastructure-less networks or having no centralized control to support the network. The nodes in mobile network communicate with each other via wireless links and they can move freely in the network. Hence, the network topology changes. Routing as one of the main function of any network including MANETs. It is needed whenever data packets need to be transmitted to the destination nodes through various other nodes. Each node in the network is responsible for transferring packets to the destination i.e. each node is capable of performing routing functionalities. MANET is a multi hop network as data has to be routed through multiple hops. In order to achieve an acceptable performance in such an environment, routing protocols should be robust against both the dynamic nature of the environment that may cause the existing links and the paths to break after a while as a result of mobility of nodes in the network, and possibility of the malicious nodes that try to disrupt the network. [3]

In MANETs, each intermediate node acts as a router and responsible for forwarding of packets to the next hop or communicating with some other nodes. This creates many susceptibilities in the network layer. For example, routers can become malicious and do not intentionally forward data to the other nodes.

Some nodes may also be malicious in sense that they advertise the false routes in order to prohibit forwarding of data to the other nodes. Some type of attacks includes flooding the network with so many packets and jamming the network in order to avoid others to use the network or consuming the network resources. So, security in ad hoc network is a major concern. Each protocol must be designed keeping in mind the security concerns in order to provide secure transmission over the network.

Many routing protocols have been designed for MANETs. Most of the routing protocols in MANETs are either On Demand or Table based. These are Dynamic Source Routing (DSR), Ad Hoc On Demand Distance Vector (AODV) protocols, DSDV (Destination Sequenced Distance Vector) routing protocol, etc. These routing protocols assume that all the nodes in the network are cooperative and trustworthy. But as in MANETs, all the nodes are free to enter or leave the network; they can freely communicate to other nodes as well. So, secured transmission of packets is a major concern.

Securing a network is to provide authentication, confidentiality, secured transmission of data without loss of the functionality, detection of the malicious nodes and to make a secure path over the nodes in the network. The main security attributes are: availability, confidentiality, integrity and the authentication. This paper presents a new technique DDBA-DSR for detection against the deep black hole attack. II describes the basic functionality of the DSR protocol. III describes the literature survey on DSR protocol. Part IV describes the deep black hole attack and part V describes the proposed work in which algorithmic steps are given and then, in part VI simulation is done and finally part VII concludes the paper.

2. OVERVIEW OF DSR PROTOCOL

One of the most popular on-demand routing protocol is dynamic source routing protocol (DSR) in which a node attempts to discover a route to some destination only when it has a packet to send to that destination. DSR consists of two phase: route discovery and route maintenance. Route Discovery is the process of finding the route from one node to another i.e. source to destination, while Route Maintenance is the process of finding the broken links in the network and managing the previously discovered routes. [10]

Route Discovery is divided into two stages: Route Request (RREQ) and Route Reply (RREP). Whenever a node wants to communicate in the network and does not have a route in its Route Cache to the destination, it broadcasts a RREQ message to get a route. Each neighbor receives the RREQ and checks in its own cache for the route. If the requested route is not present in its cache, then the node adds its own address in the address list in the packet and rebroadcast it. This process continues until either the maximum hop counter is reached or the destination is reached. When the destination node receives the RREQ packet, appends its address and generates a route reply packet (RREP) and send towards the source using the reverse of the list of the nodes in RREQ. Unlike RREQ, RREP moves towards the source of the route. When the source node receives RREP, it first stores the route in its Route Cache and then sends data packets through that route.

In Route Maintenance phase, when data is being transmitted and an intermediate node detects that the network topology has changed or the data can't be transmitted to its next hop, it generates a route error packet indicating that the next hop is unreachable; it also appends its own address in the packet and send it towards the source node. All the nodes getting this information in the route also modifies their route cache by deleting that node from the route list and the source node after getting this information, modifies its route cache and sends the data packets over another route.

3. RELATED WORK

For security in MANETs, many routing protocols have been designed based on the DSR protocol in order to provide protection against the possible attacks. In our work, we have implemented a new scheme DDBA-DSR for security in the DSR (Dynamic Source Routing) protocol. The secured routing protocols designed based on the DSR protocol are:

ARAIDNE[1], is a DSR-specific security mechanism based on earlier TESLA (time efficient stream loss-tolerant authentication)[2,4] protocol and symmetric cryptography has been used in all messages. Ariadne's security is based on message authentication code (MAC) and loose time synchronization is achieved from TESLA schemes used are:- (i) shared secret keys between all pairs of nodes. (ii) Shared secret keys between communicating nodes combined with broadcast authentication. (iii) Digital signatures. Authentication is achieved by sharing secret keys between each pair of nodes and the shared secrets between communicating nodes. For broadcast authentication, ARIADNE uses TESLA authentication protocol which is broadcast authentication procedure requiring relaxed time synchronization. It consists of two steps (i) authentication of routing messages. (ii) Verification that there is no node missing in the routing message headers. The protocol prevents attacker or compromised nodes from modification, fabrication and spoofing due to its authentication and routing message header features and also prevents many types of DoS attacks.

SRP[5], secured routing protocol is a part of SMT(secured message transmission)[11] protocol used for route discovery phase of SRP/SMT suit proposed by Papadimitrators and Hass.SRP assumes a security association between two communicating nodes. Source initiates a rote discovery by constructing a Route request packet identified by a query sequence number and a random query identifier (generated randomly for each route request query initiated by the source). The query id is monotonically incremented for each route request initiated by the source for the destination, four billion such id are possible and it is reset when the SA is established between two authenticated nodes to communicate.

- It has been found that rushing attack cannot disrupt the route discover phase of SRP and malicious nodes cannot fabricate requests.

SRP[6], prevents spoofing attack and vulnerable to wormhole attack. Intermediary nodes are not authenticated and invisible node attacks.

SADSR[7], a secure routing protocol for mobile ad hoc networks. In SADSR, messages are authenticated using digital signatures based on cryptography. The basic idea behind SADSR is that multiple routes are there to each destination and a trust value is stored for each node in the network. Each path is assigned a trust value based on the trust values of the nodes on the path. Those paths are preferred having higher trust values.

endairA[8] deals with securing routing protocols of MANETs against packet dropping misbehavior. ENDAIRA is similar to the last version of ARIADNE protocol. In this, route reply packets are signed instead of route request ones by applying digital signatures. All the secure routing protocols are vulnerable to black hole attack. The 1st solution dealing with packet dropping problem was watchdog. CORE and CONFIDANT are among solutions that mitigate this problem by defining some reputation and punishment strategy.

[9]endairA was later proposed using TIK (TESLA with instant key disclosure) protocol. It prevents adversarial nodes from impersonation, forging, deleting any node from the node list carried by the RREP packets or even rendering them.

RSRP[12], an efficient protocol in which a broadcast authentication scheme is presented. this scheme provides authentication and doesn't need any clock synchronization. This secured protocol authenticates the sender and receiver of the message, route error messages can't be forged, doesn't broadcast replayed route requests, much less vulnerable to DoS attacks and ensures the integrity of nodes listed in the source route.

S-PDSR[13] proposes enhancements in Preemptive DSR to provide secured route discovery. This protocol evaluates integration of Secured Routing Protocol (SRP) and Secured Message Transmission (SMT) with Preemptive Dynamic Source Routing (PDSR) to get Secured PDSR(S-PDSR), which is capable of secured route discovery. No security association is there in P-DSR.PDSR also needs a random id of traversed nodes in the route request packet. At destination, it firstly verifies the authenticity of the packet, by calculating MAC. S-PDSR retains the basic functionality of PDSR and integrates the security aspects based on SRP. The secured route discovery of multiple routes is achieved in S-PDSR with minimum modifications in the methodology of PDSR and SRP.

ARAN, authenticated routing for ad hoc networks. It is based on some query-reply dialog. ARAN introduces authentication, message integrity and non-repudiation.

- Minimal performance cost
- Modifications attacks are prevented
- DoS attacks go undetected as it cannot differentiate between legitimate and malicious RREQs coming from authenticated nodes.
- Doesn't protect against attacks that are conducted by authenticated selfish nodes.

In ARAN[15], the attacks of integrity and non-repudiation are mitigated using the public key cryptography scheme. Conclusion is that the protocol results in a route disruption, route diversion or creation of incorrect routing state and also vulnerable to the wormhole attack.

ARAN doesn't attempt to continuously maintain the up-to-date topology of the network, but rather when there is a need , it invokes a function to find a route to the destination and also doesn't authenticate the selfish nodes. So, a reputation based scheme called reputed-aran[14] was proposed to detect and defend against selfish nodes.

ADSR [16], this protocol employs elliptic curve cryptography to sign the route discovery packets. It also uses the aggregate signature scheme which allows us to connect M signatures of M different signers, in one single signature. Its drawback is that checking would have to be done in blocks.

e-ARAN [17], e-ARAN was designed to detect and handle authenticated selfish nodes, based on reputed OCEAN scheme. Offers authentication, confidentiality, message integrity and non-repudiation by utilizing certificate infrastructure. It protects the network against fabrication, modification, spoofing and denial of service attack. Schemes used are currency based scheme and reputation based scheme.

A Temporal table Authenticated Routing Protocol for Ad hoc networks[18], In this, temporal table based techniques are applied on the ARAN protocol to detect selfish nodes and improve the performance. ARAN–authenticated routing protocol is a secure protocol which provides security for attacks using modification, fabrication, impersonation and securing shortest paths[19].In[20], Marti et al, proposed a scheme that contains two major modules, termed as Watchdog and Path rater to detect & mitigate respectively. As it rely on overhearing, the Watchdog may fail to detect misbehavior of the node or raise false alarms. CONFIDANT Scheme observes the next hop neighbors behavior using the over hearing technique. This scheme causes same problems as the Watchdog Scheme. S.Bansal et al, proposed an observation based Co-Operation enforcement in Ad hoc Networks (OCEAN) [21].In contrast to CONFIDANT, OCEAN avoids in direct (second hand) reputation information & uses only direct first hand observation of other nodes behavior. Temporal table is more efficient and more secure than ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes.BDA-DSR[23], a protocol that proposed a scheme that detects and avoids the black hole node in the network before the actual routing starts by using fake RREQ packets. The protocol is an extended version of DSR. The fake RREQ packets are send before the routing process starts in order to identify the malicious nodes. This mechanism is performed before actual routing so that network is protected against the damage due to the malicious nodes.in this, an acknowledgement scheme is also used, in which data packets are routed only after receiving the acknowledgement by the source node. This process of sending fake RREQ packets for finding the black hole nodes in the network is similar to the actual DSR RREQ packets. The only difference is that the destination address used is fake i.e. invalid address which really does not exist and only live for a certain time. When source node receives reply for this fake RREQ, it checks for the node that initiated this packet and records the address of that node in the list of malicious nodes. After that, normal DSR routing process is started.

The protocols given above provides authentication, integrity, some protects against the DoS(Denial Of Service) attacks, non-repudiation, some presented schemes to protect against wormhole attack like using TESLA scheme and secured message transmission scheme is also provided. There is also a protocol that protects against blackhole attack.

But [22] introduces a new attack named deep blackhole attack that not only introduces fake RREP for the RREQ packets but also interrupts and modifies the valid RREP originated from the target node. So, our proposed work is to provide a method to protect against deep black hole attack.

4. DEEP BLACK HOLE ATTACK

In [22], a new attack was proposed named deep black hole attack. This attack generates fake RREP more strongly than black hole attack. Deep black hole attack is an extended black hole attack. The only difference is that deep black hole attack introduces fake RREP in response to the RREQ generated and the overheard RREPs.
Deep Black hole attack, like the black hole attack, includes both fake RREP advertisement phase and packet drop phase. In its advertisement phase, the deep black hole node generates fake RREPs in response to received RREQs and also in response to the overheard RREPs. These overheard RREPs carry the source route that is generated by another node with its modification. The attacker node overhears the route that is passing over the network within its transmission range and using that source route, it generates a new RREP packet that is fake and forwards it to the source node. This new fake route is almost shorter than the main route and includes malicious node itself as a hop in the route. As a result, the nodes that receive fake RREPs often use them to send their data packets in the future. Finally, when data packets are sent through this node to the malicious node, the malicious node discards all the data packets silently and makes it unable to reach to its destination.
Consequently, the Deep Black hole attack's operation can be summarized as follows:

- Advertisement phase
  - Fake RREP in response to RREQ
  - Fake RREP according to overheard RREP(new)
- Packet Drop phase

The black hole and the deep black hole attack differ only in the route advertisement phase. Sending fake RREP

according to the overheard RREP has been added to the original black hole.

5. PROPOSED WORK

The proposed work is to present a DSR based secured routing protocol. The proposed work is to protect the network against the deep black hole attack. Our proposed work is about to perform the secure communication over the blackhole nodes.

The presented work is divided into two phases. The first phase is to setup the criteria for the bad (blackhole) nodes and the second phase is to perform the communication over a safer path. In this presented work, a dynamic data mining approach is defined to identify the safe node for communication over the network. Initially the transmission will be performed in normal way, but after specific time interval, the throughput and the network delay is been analyzed and communication association is also analyzed between each pair of nodes. The nodes will be analyzed in terms of reply received from the node and the address of the node will be checked and also, for analysis, we have defined a minimum eligibility criteria called support value at 50% throughput rate and 50% of the normal delay. The best nodes are identified with the confidence level of 90% throughput and 10% of delay. As the communication will be performed, both the delay over a node and the throughput is analyzed over the communicated nodes. And the data is transmitted over a safer path.

Algorithmic Steps for DDBA-DSR

- Setup the network with N nodes under defined parameters.
- Define the multiple sources called S1,S2…Sn and multiple destination nodes called d1,D2…..Dm
- Define the Minimum Throughput Support and Confidence called EffectiveSupport and EffectiveConfidence. Also define supportdelay and confidencedelay
- For i=1 to n

For j=1 to m

S(i) will broad cast the Fake RREQ Each node, node1, node2, node3……..node k receive the request and perform the following consideration before sending the RREP.

If

(TypeofPacketReply(RREP) =Data)

Drop RREP;

ElseIf

(TypeofPacketReply(RREQ))

Generate Route Reply FRREP;

ElseIf

(OverHeard(RREP)=True)

Generate new FRREP;

Else

Estimate the Association mining between each intermediate nodes under different parameters for all k nodes called Throughput, IdleRate and the network delay etc.

If

(PerformRREQ(Node(i))=True)

If

(Throughput(Node(i))> EffectiveSupport and RREPTime (Node(i))<supportdelay)

If

(Throughput(Node(i))>Throughput(Node(i+1) And IdleRate(Node(i))> IdleRate(Node(i+1))

If

(Throughput(Node(i))> EffectiveConfidence And RREPTime(Node(i))<confidencedelay)

Generate RREP so that the node is valid node.

Set Node(i) as Valid Path Node.

ElseIf

(Throughput(Node(i))>EffectiveConf idence)

Generate RREP so that the node is valid node

Set Node(i) as Valid Path Node

Else

Mark the Node as MaliciousNode

Reconsider Node(i) if No node is under confidence level

Else

Mark the node with DeepBlackhole Attack and Block it

Avoid Node (i) from path

In this present work, a hybrid mechanism is presented that will perform the detection as well as the prevention to these kind of attacks. The detection mechanism is here defined relative to the fake message identification. According to this, the blackhole node is not aware about the Fake request. In such case, for the detection process a fake request is broadcasted, the node that will reply for this fake request will be identify as the blackhole node. To perform the prevention process, a neighbor node analysis is performed for each node between the communication paths. The analysis will be performed under three main parameters called packet loss, response time and the packet delay. This analysis will be performed on the neighbor nodes of current node. If a node having the higher loss and higher communication delay will be presented as the black hole node. But to perform the second level analysis, the communication of this expected blackhole node is performed with all neighbors under the defined threshold values. If the node not replies to any of neighbor node, the node will be set as the blackhole node. The neighbor node that will provide the least throughput and provide the lower delay will be selected as the next neighbor. This preventive path will be generated till the destination node not arrived. In this way, we have generated a new scheme called DDBA-DSR. This protocol performed better in terms of packet loss and packet delay and also in avoiding data transmission through black hole nodes.

6. SIMULATION AND ANALYSIS

6.1. Simulation Model

To compare the proposed secured routing protocol with DSR protocol and to check the effectiveness of the proposed method, a network scenario of 26 nodes has been taken for experiment. Area that we used for implementation of networks is 700m * 700m. A source node and a destination node is selected and data packets of size 512 bytes each are transmitted from source to destination. Table 1 shows different simulation parameters and their associated values.

Table 1: Simulation Parameters

Parameter Name	Value
Propagation type	TwoRayGround
No. of nodes	26
Routing protocol	DSR
Simulation area	700x700
Traffic type	CBR
Packet size	512 B
Simulation time	100s
Data rate	125 packets/sec

6.2.Performance Evaluation

We have used the ns2 network simulator to analyze and evaluate the performance of the DDBA-DSR protocol. The analysis of the work is performed under different parameters such as packets transmitted, lost and the delay rate.

6.2.1. Packet Drop Ratio

A comparison of the DSR protocol in presence of Deep Black hole and the DDBA-DSR is given in terms of packet drop ratio. Deep Black hole absorbs more network traffic and, as a result, drops more packets. Point to point packet drop ratio in case of deep black hole attack is more as compared to DDBA-DSR.

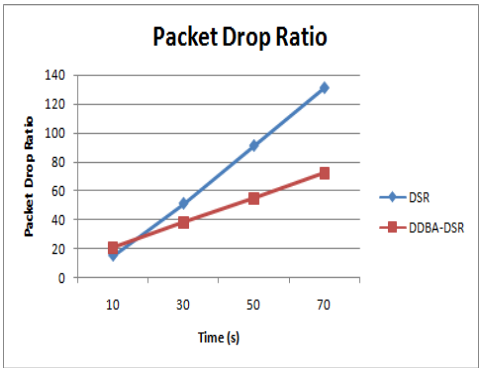

Fig. 1: Comparison of DSR and DDBA-DSR in terms of packet drop ratio

6.2.2. End-to-end delay

In Fig. 2, end-to-end delay is plotted for both scenarios. The amount of delay for has reduced compared to DSR protocol having deep black hole. It should be noticed that such parameter is calculated just for packets which have received to their destination; and no delay is calculated for dropped packets.

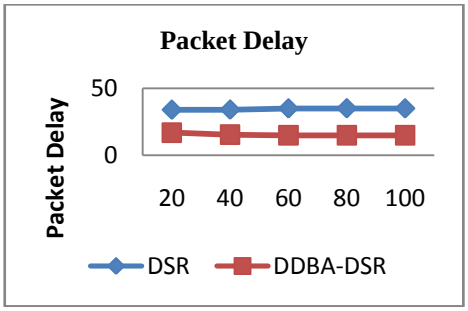

Fig. 2: Comparison of DSR and DDBA-DSR in terms of packet delay

6.3.3. Network Throughput

Network throughput is the average rate of successful delivery of messages in the network and measured in bits per second [23](bps).Figure3 represents the comparison between the original DSR in presence of deep blackhole attack and the DDBA-DSR protocol.

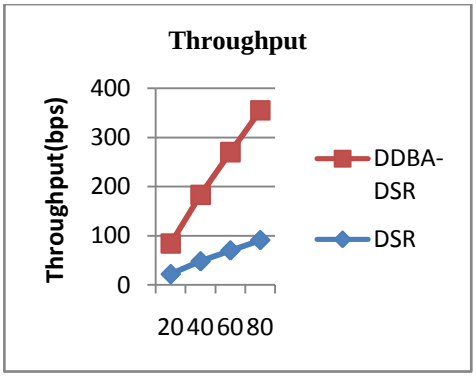

Fig. 3: Comparison of DSR and DDBA-DSR in terms of throughput

6.3.4. Number of routing packets

The Black hole nodes generate and propagate numerous optimum fake routes. As a result, other nodes in such attacks send smaller number of RREPs compared to selfish nodes and there are less number of routing packets that are transmitted. Besides, sending fake RREPs prevents diffusion of many of RREQs by ordinary nodes. Figure 4 represents the comparison of DSR and DDBA-DSR in terms of routing packets.

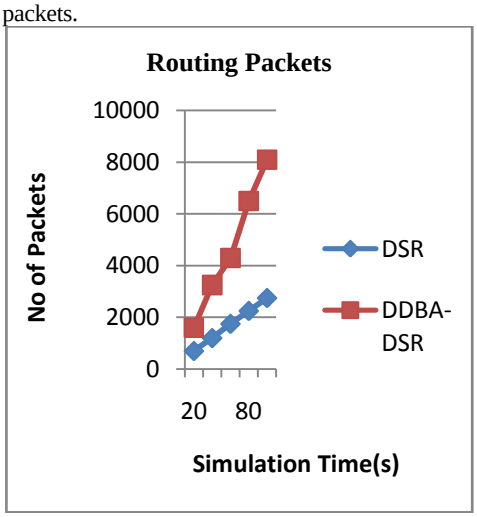

Fig. 4: Comparison of DSR and DDBA-DSR in terms of routing packets

Figure 5 represents the comparison of packet loss between DSR and DDBA DSR.

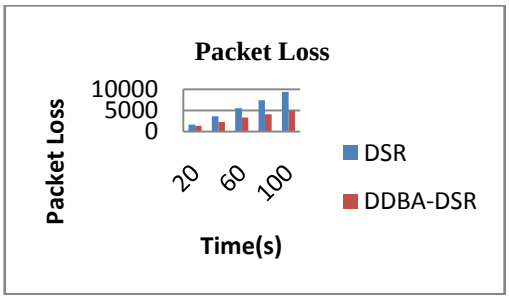

Fig. 5: Comparison of DSR and DDBA-DSR in terms of packet loss

Simulation and analysis shows that DDBA-DSR performed better in terms of the above mentioned parameters.

7. CONCLUSION

The security is one of the major issue in mobile ad hoc networks because the network is publicly available so that any user can enter to the network system. Routing protocols in MANETs are prone to many attacks. One of such attacks is the deep black hole attack. In this paper, a method is presented to protect against the deep black hole attack in the network. Simulation is performed in NS2 simulator and the simulation results showed that the proposed work has improved the communication and reduced network delay and the communication. The presented work also performed better in terms of packet loss. As a future work, it can be extended for other security attacks also by applying proper encryption schemes. Or the work can be done against the selfish nodes that are registered as a legitimate user.

8. REFERENCES

[1] Yih-chun huand Adrian Perrig, David.B.Jhonson "Ariadne: A Secure On-Dem-and Routing Protocol for Ad Hoc Networks" 2005 Springer Science+ Business Media, Inc. Manufactured in The Netherlands.

[2] A. Perrig, R. Canetti, D. Song and J.D. Tygar, Efficient and secure source authentication for multicast, in: Proceedings of the Network and Distributed System Security Symposium, NDSS'01 (February 2001) p. 35–46.

[3] C.E. Perkins (Ed.), Ad Hoc Networking, Addison-Wesley Longman, 2000.

[4] A. Perrig, R. Canetti, J.D. Tygar and D. Song, Efficient authentication and signing of multicast streams over lossy channels, in: Proceedings of the IEEE Symposium on Security and Privacy (May 2000) pp. 56–73.

[5] Ani1 Rawat, P. D. Vyavahare, A. K Ramani, "Evaluation of Rushing Attack on Secured Message Transmission (SMT/SRP)protocol for Mobile Ad Hoc Networks", 0-7803-8964- 6/05/$20.M1 Q z IEEE.

[6] Huabing Yang, Xingyuan Zhang, and Yuanyuan Wang "A Correctness Proof of the SRP Protocol" 1L-4244-0054-6/06/$20.00 ©2006 IEEE

[7] Shayan Ghazizadeh, Okhtay Ilghami, Evren Sirin, Fusun Yaman "Security Aware Adaptive Dynamic Source Routing Protocol" Proceedings of the 27th Annual IEEE conference on Local Computer Networks (LCN.02) 0742-1303/02 $17.00 © 2002 IEEE

[8] Djamel Djenouril, Othmane Mahmoudil, Mohamed Bouamamal, David Llewellyn-Jones, and Madjid Merabti "On Securing MANET Routing Protocol Against Control Packet Dropping" 1-4244-1326-51071$25.OOI©B2007 IEEE.

[9]A.F.A. Abidin, N.S.M. Usop "An Analysis on Endaira: A Provably Secure On-Demand Source Routing Protocol" A.F.A. Abidin et al. / (IJCSE) international Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 437-442

[10] David B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts". In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pages158-163, December 1994.

[11] P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile Ad hoc Networks", Elsevier Ad Hoc Networks Journal, vol. 1, no. 1, pp. 193-209, July 2003.

[12] S R Afzal, Subir Biswas, J.B Koh, Taqi Raza, Gunhee Lee, and Dong-kyoo Kim, "RSRP: A Robust Secure Routing Protocol for Mobile Ad hoc Networks" 1525-3511/08/$25.00 ©2008 IEEE.

[13] V. Ramesh, Dr. P. Subbaiah, N. Sandeep and C. P. Bhaktavastalam, "Secured Preemptive DSR(S-PDSR): An integration of SRP and SMT with Preemptive DSR for Secured Route Discovery", international Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, September 2010.

[14] Abdalla Mahmoud, Ahmed Sameh Sherif El-Kassas" Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN)" 0-7803-9466-6/05/$20.00 ©2005 IEEE

[15] Davide Benetti Massimo Merro Luca Vigan`o "Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endairA" 978-0-7695-4153 -2/10 $26.00 © 2010 IEEE DOI 10.1109/SEFM.2010.24

[16] José Luis Tornos, Joan Josep Piles and José Luis Salazar "DSR: Authenticated DSR" 2011 6th International Conference on Risks and Security of Internet and Systems (CRiSIS) 978-1-4577-1891 5/11/$26.00 ©2011 IEEE

[17] Ajay Jangra, Shalini "e-ARAN: Enhanced Authenticated Routing for Ad Hoc Networks to handle Selfish Nodes" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[18] R. Sudha, S.Lecturer, CSE, Dr. D.Sivakumar "A Temporal table Authenticated Routing Protocol for Ad hoc networks" 978-1-4577-18946/11/$26.00©2011 IEEE

[19] Seema Mehla et. al. / (IJCSE) International Journal on Computer Science and EngineeringVol. 02, No. 03, 2010, 664-668

[20] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks". Proceedings of MOBICOM, August 2000.

[21] S. Bansal and M. Baker. Observation-based Cooperation Enforcement in Ad Hoc Networks. http://arxiv.org/pdf/cs.NI/0307012,July 2003

[22] Mahmood Salehi, Hamed Samavati and Mehdi Dehghan, "Evaluation of DSR Protocol under a New Black hole Attack", 20th Iranian Conference on Electrical Engineering, (lCEE2012), May 15-17,2012, Tehran, Iran, 978-1-4673-1148-9/12/$31.00©2012IEEE

[23] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi and Mohammad S. Obaidat, "Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks" 978-1-4673-1550-0/12/$31.00 ©2012 IEEE