www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5, May 2014, Page No. 5744-5751

A Novel Scheme for Intrusion Detection & Anticipation of Black Hole & Gray Hole Attacks In AODV Based MANET using ZED

Arti Tiwari[1], Prof.Nilmani Verma[2]

[1]M.Tech Scholar, Department of CSE, MATS University, Raipur, India
arti.tiwari01@gmail.com

[2]Assistant Professor, Department of CSE, MATS University, Raipur, India
nilmaniv@matsuniversity.ac.in

Abstract: ***Mobile Ad hoc Network typically identifies an activity of Network elements through which combine to create a network requiring no preset infrastructure. Security would be the most commonly cited issue about wireless Ad hoc system. Wireless communities pose distinctive security issues. The Brand new Security Design for mobile Ad hoc network protects the information from a number of securities threats and as well leads to very much low computational complexness. The discovery of problems where these kinds of destructive node is present will make it easy for us to prevent that attack for much more transmission. This gives a proper technique to detect this particular malicious attack for example Black hole & Gray Hole. The actual propose Technique First safeguard the system from repudiation i. e. prevents generally sender or possibly receiver simply by denying affecting sending or receiving a data offer using Zero Knowledge Protocol (ZKP) for the reason that Authentication Structure to create certain the actual authenticity in the sender node. The device also used to detect Cloning Attack. Next, if an additional attack comes about the structure is helpful to providing a fix for discovery & decline of destructive attacks utilizing Extended Data routing Info (EDRI) table along with routing stand of AODV. In addition, it maintains a brief history of previously malicious node with regard to gray behavior. The EDRI procedure is displayed but just isn't implemented within NS-2 to supply a valuable performance element such as-Packet Delivery Ratio, Packet Deliver Rate by Number of Nodes, Latency, Average End to End Delay.***

Keywords: MANET Secure Routing, Attack Detection, EDRI table Zero Knowledge Protocol.

1. INTRODUCTION

A good ad-hoc network can alter its form with respect to the work on hand. A MANET is usually an infrastructure-less circle including things like list of nodes in mobility or even mobile devices wishing to converse with each other via discussed wireless medium. This doesn't need virtually any centralized management and as a consequence, line of safeguard will be rather unclear. Each node possesses restricted conversation assortment within the network plus its node acts to be a router to ahead packets to a different node. It's rapidly deployable as well as very adaptive within Mother Nature. Nodes get substantial range of motion as well as conversation is done via airwaves sent out medium. Thus, MANETs are traditionally used within programs such as military services conversation through soldiers, robotic battlefields, crisis management teams to recovery, research through police force or even hearth fighters, substitute of preset facilities within event of earthquake, massive amounts, hearth and so forth., more quickly having access to patient's information via medical center databases regarding record, reputation, prognosis while in crisis conditions, out of the way receptors for climate, voting techniques, sports stadiums, portable office buildings, motor research, electronic digital obligations via everywhere, education techniques together with set-up of personal classes, discussion group meetings, fellow to fellow report sharing techniques [1]. The particular characteristics of MANET in addition to range of motion as well as airwaves sent out medium contributes to a number of important concerns for MANETs such as IP handling, airwaves interference, redirecting methods, electrical power constraints, stability, range of motion management, program development, bandwidth constraints, Quality of Service (QoS), and so forth. [2].

Even though options that come with MANETs entice large applicability, additionally they manifest vulnerability. This kind of vulnerability in order to attack imposes unreliability, a condition of which is not jeopardized specially inside unexpected emergency conditions. There can find a range of attack which the MANETs face. This violence could be categorized seeing that active and also passive attack. In active attack the actual enemy smashes in to the process which is capable to embed and also capture transmissions hence enhancing or perhaps

corrupting the data while inside passive attack the actual enemy basically listens for the targeted traffic and also ingredients information coming from the actual transmissions. The increasing fee and also magnitude connected with black hole attack elevate issues to get a preventive process that has the actual houses of being preventive in addition to medicinal. Therefore this specific report can be an attempt to defend against "Black hole" attack of which compromises consistency in the sites by means of shedding most info packets routed in direction of them.

Among almost all investigation concerns, however, on the list of necessary investigation concerns within MANETs will be stability; Denial-of-Service (DoS) violence is a important type of hazard currently. A couple of the extremely widespread DoS violence are Gray hole as well as Black hole attack within MANET. Within Black hole Attack, the detrimental node produces as well as propagates fabricated redirecting information as well as markets themselves seeing that creating a good speediest approach to the most likely going node [3]. If the detrimental node responses to the asking for node prior to the legitimate node responses, a new false course will be produced. Thus, packets tend not to reach on the specified vacation spot node; as a substitute, the detrimental node intercepts the packets, falls these and therefore, network traffic will be ingested [4]. Gray hole Attack is usually an file format of Black hole Attack where a detrimental node's behavior will be remarkably unpredictable. A node may well act maliciously for any particular period, but afterwards this plays its part much like different normal nodes. Both Black- hole as well as Gray hole Attack disrupt course development process as well as weaken network's functionality [5].

The remainder of paper is organized as follows. Section 2 describes interrelated work. In Section 3, Proposed Scheme is discussed for making MANET free from the Gray hole/Black hole attack. Theoretical Analysis of the Proposed Scheme is covered in Section 4. Finally Conclusion and Future guidelines are given in Section 5.

2. RELATED WORK

S. Banerjee [6] tackled two varieties of routing attacks namely Gray hole attacks and Black hole attack which reveals packet forwarding misbehavior. This cardstock presents a new mechanism able to detecting in addition to removing these malicious nodes launching these types connected with attacks. This method consists of algorithm which works the following. Instead connected with sending the overall data traffic at the same time,it divides the overall traffic directly into some little sized hindrances. So that will malicious nodes might be detected in addition to remove between the transmissions of a couple such hindrances by being sure an end-to-end examining. Source node posts a prelude message towards destination node before start of sending just about any block to be able to alert it in regards to the incoming information block. Flow with the traffic is actually monitored because of the neighbors with the each node from the route. As soon as the end with the transmission desired destination node posts an acknowledgement with a postlude message containing this no connected with data packets obtained by desired destination node. Source node use this information to check whether the data burning during transmission was in the tolerable range, or else then the original source node initiate the process of discovering and taking away malicious node by means of aggregating this response from the monitoring nodes as well as the network. Last but not least proposed a new feasible alternative for detection and removing of chain of cooperative black color and dull hole episode in AODV method. In this particular solution each node could locally maintain its very own table connected with black listed nodes whenever it will try to send data to be able to any desired destination node and additionally, it may aware this network in regards to the black listed nodes. This directory malicious nodes might be applied to find out secure trails from supplier to desired destination by steering clear of multiple black/ gray hole nodes operating in assistance.

S. Ramaswamy,[7] H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard paper offered an algorithm during which claims to prevent the cooperative black hole attack in ad-hoc circle. In this kind of algorithm every node maintains an extra Data Routing Information (DRI) table. Whenever a node (say IN) taken care of immediately a RREQ it send the id involving its next hop neighbors (NHN) in addition to DRI access for NHN towards the source. If IN seriously isn't a trustable node for source next source sends yet another route request (FRq) to help NHN. NHN in turn responds using FRp concept including DRI access for IN, the subsequent hop node involving current NHN, and also the DRI entry with the current NHN's subsequent hop. If NHN is usually trusted node next source investigations whether IN can be a black pit or not when using the DRI access for IN replied by means of NHN. If NHN seriously isn't trustable node next the same cross checking will likely be continued using the next get node involving NHN. This cross checking loop will likely be continued until a dependable node is available. Moreover, in the event that when the network within not underneath the attack, the criteria takes additional time to comprehensive. This algorithm will depend on a have confidence in relationship involving the nodes, so because of this it cannot tackle gray hole attacks.

Siba K. Udgata, Alefiah Mubeen, Samrat L. Sabat [8] proposed a new security model to address three important active attacks namely Cloning attack, MITM attack and Replay attack. We used the concept of Zero Knowledge Protocol which ensures non-transmission of crucial information between the prover and verifier. The anticipated model uses social finger print based on s-disjunct code together with ZKP to detect clone attacks and avoid MITM and replay attack. We analyzed various attack scenarios, cryptographic strength and performance of the proposed model. In Future, we are planning to extend our work to detect the passive attacks also and evaluate performance in real time using TinyOS and Tossim.

Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang , Arjun Agrawal [9] researched the particular routing safety measures concerns regarding MANETs, identified the particular cooperative black hole & gray hole attack in

which could be fitted versus the MANET and proposed the achievable remedy on their behalf inside AODV process. expanded a good offered remedy when i. age. the particular DRI Table to be able to develop the particular EDRI Table which will be able to cater to the particular Dreary characteristics with the nodes too. This proposed remedy could be applied to

1. Discover multiple black/gray gap nodes cooperating together in the MANET; and

2. Learn safe routes via supply to be able to get away by simply staying away from multiple black/gray gap nodes performing with cohesiveness.

A new constraint of method can be how the malicious nodes have for being consecutive whilst performing with cohesiveness (which may be the most frequent scenario) for being recognized through the formula. This intends to expand our own technique in order that not for consecutive cooperating nodes could be referred to as nicely. We furthermore intend to apply this particular formula and boost that regarding successful consumption.

3. METHODOLOGY

As MANET is highly susceptible to security threats as well as routing attacks. The proposed Methodology has two parts-First protect the network from security threats by applying the Novel authentication scheme to detect clone attack and prevent the network from repudiation i.e. prevents either sender or receiver from denying of transmitting and receiving a packets/message .Thus when a packet is sent, the receiver can prove that the alleged sender in face sent the packet, similarly when a packet is received the sender can prove that the alleged receiver in fact received the packet. This can be done using Zero knowledge protocol (ZKP) to verify the authenticity of the sender node.
The solution also tackle Black hole & Gray hole attack by maintaining Extended data routing table (EDRI) at each node along with routing table of the AODV protocol. In the previous work, the EDRI algorithm is proposed but is not implemented to optimize the performance metrics such as-Packet delivery ratio, Packet deliver rate by number of nodes, Average end to end delay, Latency. So, proposing it to implement in NS2(Network Simulator2).This leads to the name of the Paper ZED i.e. ,using two techniques, Zero knowledge protocols and Extended Data Routing Information (EDRI) Table for protecting the network from various security threats as well as malicious attacks and also improve the performance of the network

3.1 Authentication Using ZKP

A. Generation of unique fingerprint for each node

The base station is actually assumed to be familiar with the topology in the network and also all neighborhood information. Before deployment, the beds base station computes the finger print per node within the network. For each node u, base section finds its neighborhood facts. In our own approach, the neighborhood Ngh(u) should satisfy ng<s, where ng is how many sensor nodes in Ngh(u), s is the effectiveness of the superimposed value X. Finger produce for sensor node u is computed by for the code words of all node v which can be in the Ngh(u). Granted a sensor node u, base section computes u's fingerprint as follows. Let Xu = Xu 1, Xu 2,..., Xu ng indicates the codeword set of the nodes in Ngh(u), where Xu i denotes the codeword regarding u's i-th best neighbor. Beyond all Xu, the boolean sum of s-closest others who live nearby of node u (Xu ohydrates), is actually computed 1st. According for the property in the superimposed s-disjunct value, the producing vector should contain one or more element that has a value 0. These absolutely no elements imply the partnership among the s others who live nearby, which represent the cultural characteristic regarding sensor node u. Motivated by simply this observation, we make use of binary counsel of the position of any zero aspect in the boolean sum of Xu s as the social fingerprint regarding u. Intuitively, the cultural fingerprint should be stronger if more information from Ngh(u) is earned during the fingerprint calculation [10] [8].

B. Implementation of ZKP

After deployment, a public key N (which is a multiplication of large prime numbers) is generated by the base station which will be shared among any two nodes that will be communicating at a given time. During the communication the sender node acts as the prover while the receiver node acts as the verifier. The base station acts as the trusted third party. Each node is assigned a fingerprint which is used as a private key (secret key) [8]

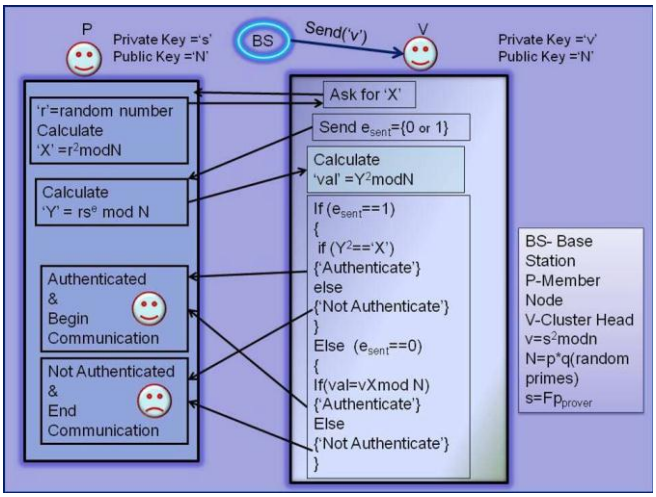

Figure 1: Implementation of ZKP

1) Stage 1: The prover P selects a random number r, calculates $r^2 modN$ and transmits to the verifier V.

2) Stage 2: The verifier V now chooses one of two questions to ask the prover P. The verifier V can ask either for the value of the product (rs) mod N, or for the value of r that the prover has just chosen. This is generally performed

by V, sending a bit *e* to P, indicating its preference of question, referred to as the challenge, such that the prover P has to provide the answer, $y = rs^e modN$, where $e \in (0,1)$. P can answer both correctly if it knows the secret s.

3) Stage 3: The prover P provides $y = rs^e \ mod \ N$ as requested and the verifier checks the result as follows. If the challenge is for e=1, the verifier expects to have recieved rs mod N. The verifier cannot presume any information about s from this, because r is a random number not known to V. Therefore, the verifier checks $y^2 modN$, which should be $((rsmodN)^2 modN)$ is the same as $r^2 * s^2 modN$. The verifier received r^2 from P in stage 1 of this round, and gets *v* from the trusted third party. If the challenge is for $e = 0$, the verifier expects to have received r, and checks that its square matches the value of r mod N provided in stage 1.
All the above three stages are discussed in Fig.1

3.2 Implementation of EDRI

A. Extended Data Routing Information(EDRI)Table:-

The *EDRI table* accommodates the gray behavior of nodes as well. Although, it gives subsequent chances to the nodes identified as black hole, it also keeps a record of the previous malicious instances of that node so that a better understanding of the node can be made and the node is given its next chance accordingly. A counter keeps track of how many times a node has been caught and the value of this counter is proportional to the time which has to pass before that node is given another chance. A node which is frequently being caught acting malicious is eventually not given a chance again.[9]

Table-1: EDRI Table at Node1

Node_id	*From*	*Through*	*Counter*	*BH*
4	0	1	1	0
5	1	1	0	0
8	0	0	2	0
10	0	0	8	1

B. Layout and Current State of the Network

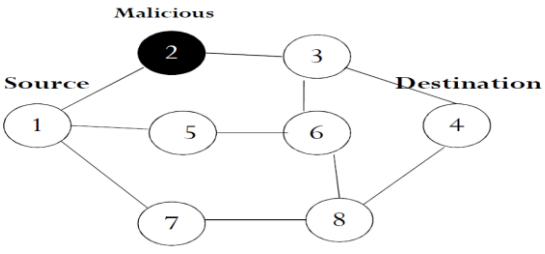

Figure 2 : Network Layout

C. EDRI Implementation Algorithm:

1.The particular destination sends out any NACK (Negative acknowledgement) across towards source by using a different route say 4-8-7-1.
2. Couple of the resource & location now mail a invigorate packet coupled the troubled route my partner and i. e. 1-2-3-4.
3. Upon this reception of any refresh bundle, a node is actually supposed to accomplish the following:
3.1. Arranged all the from and also through EDRI records to 0.
3.2. Couple of, Delete this route through its option table.
4. Complete the bundle forward.. The malicious node ignores this packet and will not forward it to a higher node. (That's the reason packets ought to be delivered from each directions so that all this nodes find it).
5.The original source node now starts this Black hole Breakthrough discovery process when using the BH_Discovery function. (discussed later)
6. Upon revealing the malicious node's identity the origin broadcasts this by giving out BHID packets.
7. Each node scars this node to become black hole (set BH area to 1) and improve the CTR price by 1.
8. Each node now starts any timer according to the CTR price, which represents time for that this concerned node will be considered malicious.
9. Right after timer expiration each node units the similar BH entry back to 0. The node continues to be given one more chance.

D. The BH_Discovery Purpose:-

1.The original source node sends RREQ bundle (Route request) intended for the very same destination.
2. Couple of, An intermediate node (IN) while using the desired route, node a couple of here, sends RREP with node username of NHN (next jump node) my partner and i. e. 3 and EDRI gain access to for NHN.
3.The original source now checks its EDRI gain access to for IN.
3.1 In the event that reliable my partner and i. e. the via entry with the node is actually 1, this uses this path and also data packets tend to be transmitted.

3.2 Couple of, Else this sends this FREQ(Further obtain packet) in order to NHN and also asks this:
3.2.1.Couple of 1. In the event that IN provides routed information through NHN.
3.2.2. Couple of 2. The subsequent hop intended for NHN inside the route.
3.2.3. Couple of 3. Possesses NHN routed data via its future hop.

3.3 NHN replies while using the FREP(Further Answer Packet) which has:
3.3.1. EDRI gain access to for IN.
3.3.2. Couple of. Next jump of NHN. (Node 5 here)
3.3.3. EDRI entry for the next jump.
3.4 If NHN is actually reliable for the source.

3.4.1. The original source checks no matter whether IN can be a black pit or not. If this through line in IN's EDRI table intended for NHN is actually 1 as well as the from line in NHN's EDRI dining room table for IN is 0, IN can be a black hole.

3.4.2. If IN can be found to become black hole, the origin broadcasts this info. (Step 7 of the proposed algorithm)

3.4.3. Else the origin updates the EDRI dining room table entries intended for IN. Data packets are now transmitted.

3.5. In the event that NHN is actually unreliable.

3.5.1. It checks whether IN can be a black hole or not. If this through line in IN's EDRI dining room table for NHN is actually 1 as well as the from line in NHN's EDRI dining room table for IN is 0, IN can be a black hole.

3.5.2. Couple of. If IN can be found to become black hole, the origin broadcasts this info. (Step 7) Else create NHN because new IN and next hop associated with NHN seeing that NHN and also go to step 3.

4. EXPERIMENTS & RESULTS

A. Performance Matrices:

Previous study elaborates the fact that diverse scientific studies used diverse metrics to evaluate functionality such as number of data packets sent along with obtained with a node, quantity of management packets dispatched along with obtained with a node, likelihood of accomplishment of an episode, expense of establishing episode and many others. In our setup of attack we've determined, right after mindful factor, to utilize this functionality metrics:

Packet Efficiency: This can be the proportion of the amount of packets obtained for the destination to the amount of packets sent on the sources. Basically, the particular tiny proportion of effectively obtained packets is called Packet Efficiency as well as packet delivery ratio.

Routing Overhead: This can be the proportion of the amount of routing standard protocol management packets carried towards the number of data packets.

Throughput: This understood to be total amount of data inside words of quantity of bytes obtained because of the destination of each next node.

B. Simulation Details

In the currently simulated scenario, we choose only one Node to be the attacker but other simulations may be performed to see the impact of having multiple attackers in the network. We collect the following information for each Time frame window at each node;

- Packet send rate
- Packet Delivery Ratio
- Latency
- Throughput

Simulator	NS-2.35
Routing Protocol	AODV
Data Flow	30% of Nodes
Number of Nodes	20, 30, 40 or 50
Number of Attackers	1
Transmission Range	250m
Simulation Time	50s
Movement Model	Random way point
Packet Size	512 bytes
Data Rates	0.5
Traffic	Constant Bit Rate (CBR)
Maximum Connections	All the nodes launch data at different time

C. Result And Discussion

In this paper we proposed a new technique for detection and prevention of Black hole and Gray Hole attacks. This technique is the combination of the Zero Knowledge Protocol and the use of EDRI table work on AODV protocol. In this section we compare the result of our technique in respect of the present AODV protocol and the comparison results shows below in term of diagram. The comparison is in term of

- Average End To End Delay
- Packet Deliver Rate-No. of Nodes
- Packet Delivery Ratio-No .of Malicious Nodes
- Latency

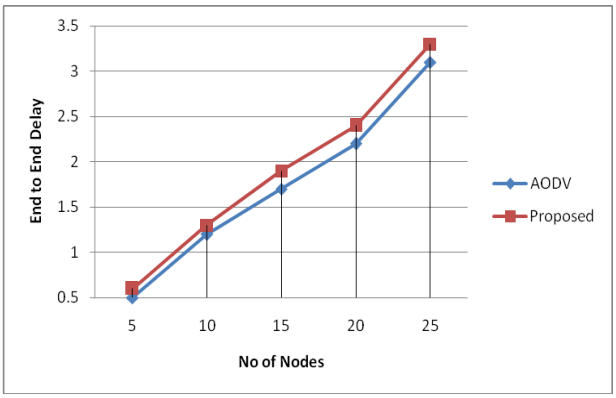

Figure 3 : Average End-to-End Delay

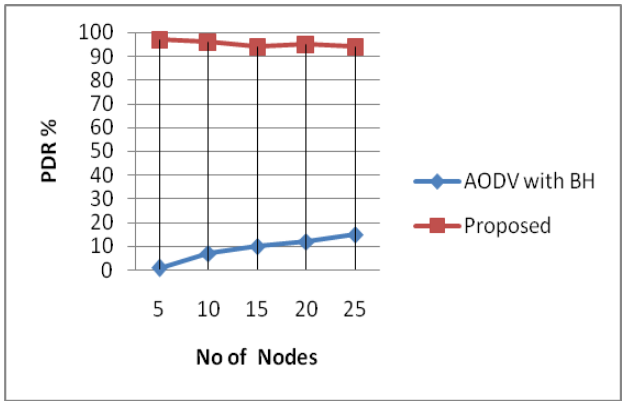

Figure 4 : Packet Deliver Rate-No. Of Nodes

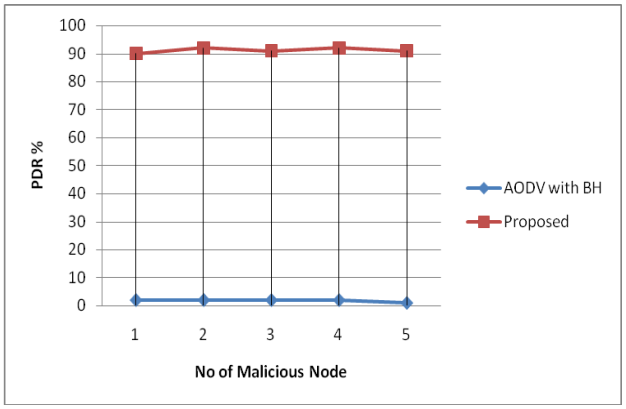

Figure 5 : Packet Delivery Ratio-No. Of Malicious Node

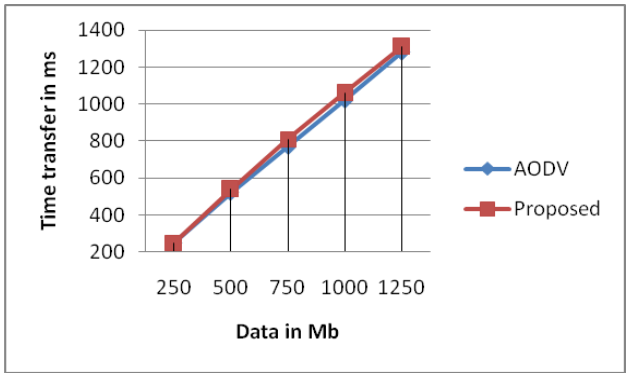

Figure 6 : Latency

5. CONCLUSION & FUTURE WORK

Black Hole and Gray Hole attack is one of the major security challenges for MANETs .The Propose solution can be applied to protect the network from security threats by first applying authentication scheme to detect clone attack and protect the network from repudiation. Secondly identify multiple black hole nodes cooperating with each other in a MANET; and Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Also expect that the effect of packet delivery ratio and Latency with respect to the variable node mobility. There is a reduction in Packet Delivery Ratio but increases in Latency. In Black hole assault all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes. The detection of malicious node in ad hoc networks is still considered to be a challenging task. The detection of Gray hole is difficult .The Propose methodology implements the EDRI algorithm to optimize the network performance. In Future,We extend the work to detect other malicious attacks such as Worm Hole, Sink Hole & Flooding attack and also compare their performances metrics with other routing protocol such as DSDV,DSR & TORA.

References

[1] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", World Congress on Engineering, 2008, pp. 219-229

[2] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[3] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[4] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Black hole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[5] Gao Xiaopeng and Chen Wei,"A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", 2007 IFIP International Conference on Network and Parallel Computing – Workshops, 2007, pp. 209-214.

[6] Sukla Banerjee Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks in Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003.

[8] Siba K. Udgata, Alefiah Mubeen, Samrat L. Sabat wireless Sensor Network Security model using Zero Knowledge Protocol for publication in the IEEE ICC 2011 proceedings.

[9] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang , Arjun Agrawa Detection and Removal of Co-operative blackhole and Grayhole Attacks in MANETs 2012

International Conference on System Engineering and Technology September 11-12, 2012, Bandung, Indonesia.

[10] Kai Xing Fang, Liu Xiuzhen, Cheng David, H. C. Du, Real- Time Detection of Clone Attacks in Wireless Sensor networks, Proceedings of the 28th International Conference on Distributed Computing Systems, 2008, Pages 3-10.

[11] Agrawal, S., Jain, S. and Sharma, S. "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of Computing, 3(1), 2011, 41-48.

[12] R. H. Jhaveri, S. J. Patel and D. C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks" 2012 Second International Conference on Advanced Computing & Communication Technologies

[13] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

[14] Ning, P. and Sun, K. "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols", Ad Hoc Networks, 3(6), Elsevier, 2005, 795–819.

[15] Hesiri Weerasinghe and Huirong Fu, Member of IEEE, "Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: "Simulation implementation and Evaluation, International Journal of Software Engineering and Its Application Vol.2, No.3, 2008. Oakland University Rochester MI 48309 USA, June 2008, pp 16-20.