INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES
ISSN: 2322-0821(O) VOLUME 9 ISSUE 3
ISSN: 2394-9910(P) July 2021 - Sep 2021
www.irjeas.org

ANALYSIS OF ENHANCED ENERGY EFFICIENT SINKHOLE ATTACK PREVENTION ON AD-HOC NETWORKS

***W. Kahlon[1], Lucas Brown[2]**

[1,2] *Department of Electronics & Communication, Deakin University, Melbourne Burwood, Australia*

Abstract- MANET is one of self-configuring fastest emerging, technology, due to commencement of economical, small & more powerful wireless devices. It is being used in most of applications, ranging from military to civilian, where each node acts as router. To facilitate communication in ADHOC network, a routing protocol is vital whose primary goal is to establish accurate & efficient route between pair of nodes, due to this lot of routing protocols have been proposed for MANET & its success depends on people's confidence in its security. In this paper we discuss an energy efficient technique of sinkhole analysis on Ad-Hoc networks.

Keywords— MANET, Ad-Hoc networks, Sinkhole attack, Router

I. INTRODUCTION

MANET is one of self configuring fastest emerging, technology, due to commencement of economical, small & more powerful wireless devices. It is being used in most of applications, ranging from military to civilian, where each node acts as router. To facilitate communication in ADHOC network, a routing protocol is vital whose primary goal is to establish accurate & efficient route between pair of nodes, due to this lot of routing protocols have been proposed for MANET & its success depends on people's confidence in its security.

The routing protocols mainly classified into three major categories as proactive, reactive & hybrid. Proactive protocols continuously learn topology of the network by exchanging topological information among network nodes. n reactive routing source node obtains path to specific destination only when it needs to send some data to it. A hybrid protocol is a combination of both reactive & proactive routing protocols [3]. Out of this AODV is a very simple, efficient, and effective routing protocol which is use mostly.

The security issue has become one of the major concerns & challenge in MANET due to its characteristics, especially for those selecting sensitive applications. In most of the routing protocols for MANET, in order to communicate beyond their transmission range nodes takes cooperation to forward packets to each other which exposes them to a wide range of security attacks, which can be classified into two types as passive & active attack, such as flooding, wormhole, black hole colluding miserly, location disclosure under which performance of AODV is already evaluated. But a sinkhole is one of severe representative attack in MANET under which AODV needs to be evaluated, where malicious node attempts to draw all network traffic towards it by broadcasting fake routing information & modify or drops packets sent for forwarding which leads to performance degradation of network.

In areas in which there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use, wireless mobile users may still be able to communicate through the formation of an ADHOC network [4]. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. Each node participates in an ADHOC routing protocol that allows it to discover "multihop" paths through the network to any other node.

The idea of ADHOC networking is sometimes also called infrastructure less networking [4], since the mobile nodes in the network dynamically establish routing among themselves to form their own network "on the fly." Some examples of the possible uses of ADHOCnetworking include students using laptop computers to participate in an interactive lecture, business associates sharing information 1during a meeting, soldiers relaying information for situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. Many different protocols have been proposed to solve the multichip routing problem in ADHOC networks, each based on different assumptions and intuitions.

A mobile ADHOC network is a self organized wireless network where mobile nodes can communicate with each other without reliance on a centralized authority. We cannot assume a trusted certificate authority and a centralized repository that are used in ordinary Public key infrastructure (PKI) in ADHOC network because nodes in a MANET can dynamically join and leave the network. All nodes can potentially be used as a router or servers. The characteristics of MANET pretense a number of challenges to security such as self configuring, wireless links, infrastructure less

© 2021 The authors. This is an open access article under the CC-BY license.

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, Volume 9 Issue 3, Jul 2021-Sep 2021, Page 16-21

nature. The characteristics make MANET good for military scenario, emergency situations, and rescue operations. But security in ADHOC network is difficult to achieve. A traditional key management service uses a certificate authority and trusted third party to issue public key certificates to all nodes in the network. This scheme is not appropriate in mobile ADHOC network due to its mobility characteristics.

The presence of a fixed supporting structure confines the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require rapid and easy deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems.

Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They propose rapid and easy network operation in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this only." Mobile ad-hoc network is a self-governing system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

Nodes in mobile ad-hoc network are free to move and arrange themselves in a random fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be varied. This allows an association of various links to be a part of the same network.

The popular IEEE 802.11 "WI-FI" protocol is proficient of providing ad-hoc network services at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet.

Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into actuality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may evenly show better performance in other places. As an example, we can imagine a group of peoples with laptops, in a business meeting at a place where no network services is present. They can easily network their machines by forming an ad-hoc network. This is one of the many examples where these networks may probably be used.

II. LITERATURE SURVEY

The infrastructure-less nature and having dynamically changing topologies, MANETs are vulnerable to many kinds of failures and attacks. Most of the attacks in MANETs target the routing protocols. The mobility of nodes makes it more vulnerable to routing protocol attacks. By attacking the routing protocols, the attackers can absorb network traffic or inject themselves into the path between the source and destination. Some latest attacks on the routing protocol in MANETs are, wormhole attack, blackhole attack, grey-hole attack, byzantine attack, rushing attack .A sinkhole attack often sets the stage for other attacks by modifying routing to improve an attacker's ability to modify packets - the routing changes often place the attacker in a position where he can receive pertinent data [3]. It is important to detect the sinkhole nodes and prune them from the MANET.

Dynamic source routing and sinkhole attack DSR [4] is one of the most widely used reactive routing protocols in ad-hoc networks. DSR uses two kinds of messages known as RREQ – Route Request and RREP – Route Reply for route discovery process. DSR starts the route discovery by sending Route Request (RREQ) packet. The Figure 1 shows the propagation of RREQ packets. The RREQ will be uniquely identified by the sequence number, source id and destination id. [4]

Node A initiates the route discovery by broadcasting the RREQ message. Each node will then add their id to the route and broadcasts it again. The nodes B, C, D are intermediate nodes and they do not have any source route to reach the node E, which is the intended destination.

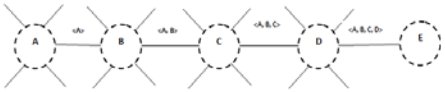


Figure 1 Propagation of RREQ

The intermediate node which has the route to the destination will send a Route Reply (RREP) and if no intermediate node has the information, the RREQ will be propagated to the destination. The Figure 2 depicts the RREP propagation from the destination node E to the source node A. Bogus RREQ will be used to carry out the sinkhole attack. If the bogus RREQ has higher sequence number than the sequence number of the original RREQ from the target node, the intermediate nodes will treat the bogus one as the latest request and discard the original one.

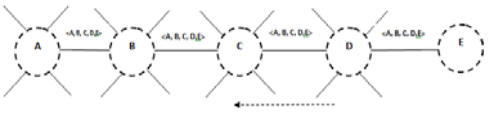


Figure 2 Propagation of RREP

Figure 3 depicts the propagation of bogus RREQ message from node A with the sequence number 888 and the target as D. By doing this, the sinkhole nodes can draw the network traffic towards them.

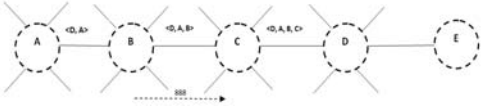


Figure 3 Bogus RREQ from node A

This can cause node failure because of the higher power consumption and the network may fail because of the heavy congestion in a particular route. So, it is imperative to detect the sinkhole nodes as early as possible and detach them from the MANET. [12]

According to Karlof and Wanger [5], the aim of sinkhole attack is to lure nearly all the traffic from a particular area of the network through a compromised node, creating a

© 2021 The authors. This is an open access article under the CC-BY license.

metaphorical sinkhole with the adversary at the centre. The malicious node attracts its neighbors by giving bogus route replies claiming to have the best path perhaps the shortest path to the intended destination. Hence, the victim nodes start sending the data packets through the sinkhole to the destination. But, sinkhole nodes may either drop the packets or perform selective forwarding making the destination node to suffer by data loss or receiving corrupted data packets. As the sinkhole attack interrupts the routing in the network, the scalability of the ADHOC network is affected in the presence of sinkhole nodes.

ADHOC network security measures can broadly be classified in to two major areas. One is the prevention method and the other is the detection and isolation method. The prevention techniques are based on cryptographic methods such as authentication, key distribution and management, encryption and decryption. According to Zhou and Haas[1], Kurian[2], Frankel et al[3] and Khalili et al.[4], the message being sent from a node to other must have been encrypted using the secret key and it would be decrypted by the destination before reading. This needs the key to be shared by the source and the destination apriori by means of any method proposed in the literature. Even if it sounds good, it is infeasible to be accomplished in the ADHOC network environment due to the absence of centralized infrastructure and the limited capabilities exhibited by the mobile nodes. Because the energy consumption is also an important factor in MANET organization, nodes cannot be expected to perform complex calculations which are very much needed for the cryptographic techniques [16], [7].

H. Chris Tseng et al. [3] proposed two sinkhole detection indicators for Mobile Ad-hoc Networks after analyzing the sinkhole problem in the context of Dynamic Source Routing for wireless mobile ad-hoc networks. The two indicators proposed are Sequence number discontinuity and Route adding ratio. To limit the number of RREQs propagated, a node only processes an RREQ if it has not already seen the packet, and its address is not present in the route record of the packet. The sequence number discontinuity is measured by the overall average difference between the current and the last sequence number from each node, plus a penalty that is proportional to the number of observed duplicate sequence numbers.

Watchdog was proposed by Marti et al. [18] to mitigate the presence of a sinkhole problem in the network. The proposed method is an extension of the Dynamic Source Routing protocol (DSR). To identify a misbehaving node, a sending node promiscuously listens to next node's transmission. If the next node does not forward the packet,then it is misbehaving. The watchdog maintains a copy of recently sent packets and compares each overheard packet with the copy of packets it holds to check if there is a match. If a match is found, the packet in the buffer deleted forever. If a certain packet is in the buffer beyond certain time, the watchdog increments a failure tally for the node which should have forwarded the packet by one. Once, that counter exceeds a certain threshold value, it concludes that the node is malicious and sends a notification to the source. However, the watchdog is vulnerable to attacks from two consecutive and cooperating attackers where the first node hides the fact that the second node did not forward the data.

Ramaswamy et al. [16] proposed a solution to identify the cooperative attack. The proposed solution has a Data Routing Information table which contains a trusted nodes list and Cross Checking. The source node uses only the trusted nodes with good transmission history for sending the data packets. If the source node doesn't have enough history of the intermediate nodes then the source node will send further a request message to the next hop after the intermediate node in order to identify the trustworthiness of the intermediate node. A good intrusion detection approach should take care of the security in all the different layers of the network. In this section the different intrusion detection techniques for sinkhole detection are discussed.

Marchang N et al. [5] proposed the collaborative technique which uses one of the mobile nodes as the monitor node. The monitor node is responsible for the detection of the malicious nodes. This is done by the voting by other nodes.

Gisung Kim et al [6] proposed the cooperative method which uses three kinds of packets namely Sinkhole Alarm Packet (SAP), Sinkhole Detection Packet (SDP) and Sinkhole Node Packet (SAP) [6]. Sinkhole Alarm Packet (SAP) will contain the sinkhole route, sequence number of the bogus RREQ, current sequence number of the node itself. Sinkhole Detection Packet (SDP) contains the common path, sequence number of bogus RREQ, network id of itself. The nodes in the sinkhole path are not allowed to generate or forward an SDP.

If any node receives an SDP from the nodes in the sinkhole path, it simply discards the packet and detaches the sender of the SDP from the network. Sinkhole Node Packet (SNP) informs the network of sinkhole node, the node broadcasts a SNP. The SNP packet will contain the sinkhole node to the whole network unless it received an SNP for this sinkhole route from another node. Cluster analysis method for sinkhole detection was proposed by Woochul Shim et al [10] which is a data mining technique. Cluster analysis works by grouping data such that objects in a given group are similar to each other and different from other groups. In this approach, cluster analysis is used to separate false RREQs from normal RREQs and to verify indicators for detection.

The hierarchical approach given here does not require predetermined numbers of groups. This approach is used because there may be more than two groups such as false RREQs or normal RREQs, etc. Cluster analysis requires distance measures to examine the differences among clusters. This approach also suffers because of the mobility of the nodes and the requirement of some controlling point.

The sinkhole detections methods using anomaly detection available in the literature is classified in to two clauses; the first clause is using the sinkhole detection indicators (SIIS) and the second on is the collaborative or cooperative methods. The following table provides a brief comparison of these methods under different parameters.

The detection methods proposed earlier are suffering with either one of the following or both of the following shortcomings. As, the mobile nodes are expected to communicate number of additional messages apart from the normal operations, they are overburdened; this results in poor performance of the mobile devices as their memory capacity and the battery power is limited; some of the

© 2021 The authors. This is an open access article under the CC-BY license.

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, Volume 9 Issue 3, Jul 2021-Sep 2021, Page 16-21

approaches need a centralized control for their detection operation which may be often infeasible in MANETs because of the mobility.

Trust is defined as a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities. Trust has also been defined as the degree of belief about the behavior of other entities or agents. The goal is to provide nodes with a mechanism to evaluate the trust level of its direct neighbors. Our model can be divided in two distinct layers learning layer and trust layer. The Learning layer is responsible for gathering and converting information into knowledge. The Trust layer defines how to assess the trust level of each neighbor using the knowledge information provided by the Learning layer and the information exchanged with direct neighbors. Both layers can interact with all layers of the TCP/IP model.

The approach presented in [1] involves the base station in the detection process, resulting in a high communication cost for the protocol. The base station floods the network with a request message containing the IDs of the affected nodes. The affected nodes reply to the base station with a message containing their IDs, ID of the next hop and the associated cost. The received information is then used from the base station to construct a network flow graph for identifying the sinkhole. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder.

A new approach of robust and lightweight solution for detecting the sinkhole attack based on Received Signal Strength Indicator (RSSI) readings of messages is proposed in [3]. The proposed solution needs collaboration of some Extra Monitor (EM) nodes apart from the ordinary nodes. It uses values of RSSI from four EM nodes to determine the position of all sensor nodes where the Base Station (BS) is located at origin position (0, 0). This information is used as weight from the BS in order to detect Sinkhole attack. The simulation results show that the proposed mechanism is lightweight due to the monitor nodes were not loaded with any ordinary nodes or BS. The proposed mechanism does not cause the communication overhead.

A novel algorithm for detecting sinkhole attacks for large scale wireless sensor networks is discussed in [4]. The detection problem is formulated as a change-point detection problem. The CPU usage of each sensor node is monitored and analyzes the consistency of the CPU usage. By monitoring the CPU usage of each node in fixed time interval, the base station calculates the difference of CPU usage of each node. After comparing the difference with a threshold, the base station would identify whether a node is malicious or not. Thus, the proposed algorithm is able to differentiate between the malicious and the legitimate nodes.

The scheme to defend against sinkhole attacks using mobile agents is proposed in [5]. Mobile agent is a program segment which is self controlling. They navigate from node to node not only transmitting data but also doing computation. A routing algorithm with multiple constraints is proposed based on mobile agents. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sinkhole attack. It does not need any encryption or decryption mechanism to detect the sinkhole attack. This mechanism does not require more energy than normal routing protocols.

III. Problem Statement

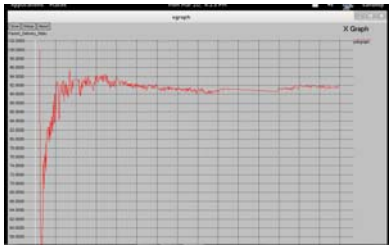
In this type of attack sinkhole node tries to attract data to itself by convincing neighbors through broadcasting fake routing information & let them know itself on the way to specific nodes. Through this procedure, sinkhole node attempts to draw all network traffic to itself. Thereafter it alters the data packet or drops the packet silently. It increases network overhead, decreases network's life time by boosting energy consumption; finally destroy the network [7].

In AODV protocol, sinkhole attack is set up by modifying sequence number in RREQ, higher the sequence number, then route will be more recent the packet contains. Sinkhole node selects the source, destination pair. It observes the source node's sequence number carefully from the RREQs of source node and generates a bogus RREQ with a higher sequence number than the sequence number of the source node. It then broadcasts the bogus RREQ Nodes.

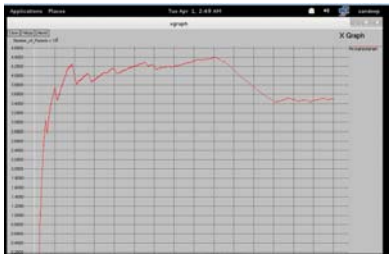
Nodes that take this bogus RREQ recognize that this route could be a better & fresh route to the source than other route. So source node sends data to destination through sinkhole, also when the nodes need to send data packets to the source node, they use the fake routes learned from bogus RREQ. Hence, the packets are concentrated in the sinkhole node.

IV. Results and Analysis

PACKET DELIVERY RATIO (PDR) GRAPH of Normal AODV



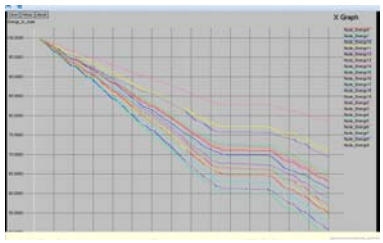
THROUGHPUT GRAPH for Normal AODV



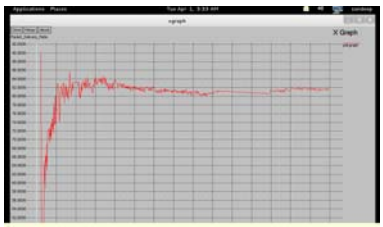
Energy Consumption for Normal AODV

© 2021 The authors. This is an open access article under the CC-BY license.

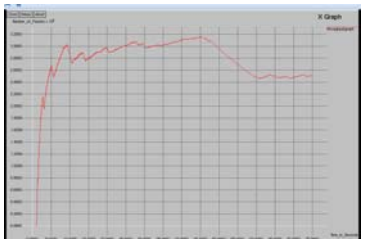
International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, Volume 9 Issue 3, Jul 2021-Sep 2021, Page 16-21



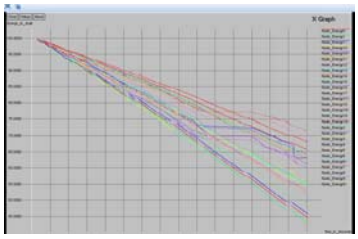
Packet Delivery Ration (PDR) on Attacked AODV



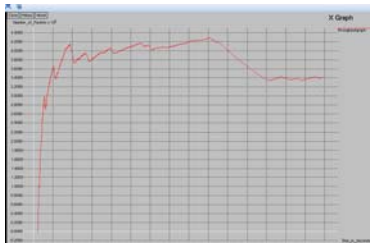
Throughput Graph for Attacked AODV



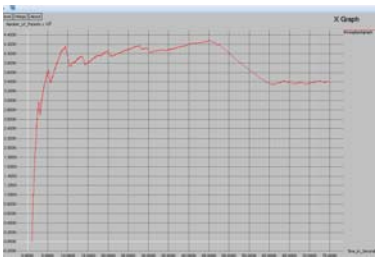
Energy Consumption Output on Attacked AODV



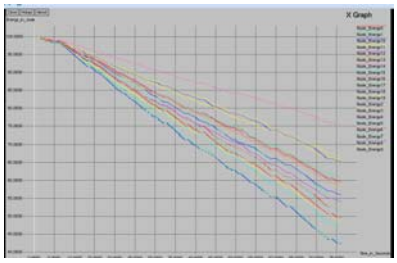
Packet delivery ratio (PDR) on Recovered AODV



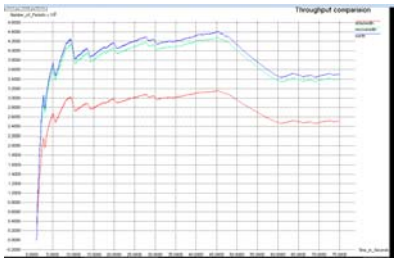
Throughput Graph for Recovered AODV



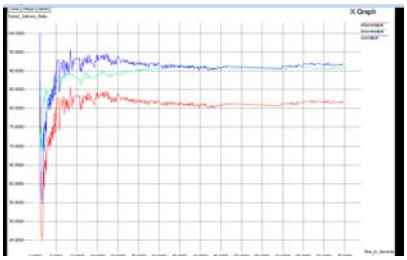
Energy Consumption Output on Recovered AODV



Results – throughput comparisons



Overall Packet delivery ratio



V. CONCLUSION

In this paper we studied various attack on routing algorithm and implement a novel An Energy Efficient Sinkhole Attack Analysis on ad-hoc Networks by making some modification and improvement on existing algorithm.

We will demonstrated that our proposed algorithm is energy efficient and load balanced thus improving overall performance of AODV routing under sinkhole attack.

Our future work will mainly focus on to analyze & study sinkhole problem on the context of other routing protocols and to evaluate variation in its performance after applying our detection & prevention mechanism by considering other performance metrics also.

© 2021 The authors. This is an open access article under the CC-BY license.

REFERENCES

[1] Elizabeth M. Royer, University of California, Santa Barbara, Chai-Keong Toh, "A Review of Current Routing Protocols for ADHOCMobile Wireless Networks", IEEE Personal Communications, pp 46-55 April 1999.

[2] Pearlman, Marc R., Haas, Zygmunt J, "Determining the Optimal Configuration for the Zone Routing Protocol", IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, pp 1395-1414 August 1999.

[3] S. Yi and R. Kravets, "Moca: Mobile certificate authority for wireless adhoc networks", Proceedings of the 2nd Annual PKI Research Workshop (PKI 2003), 2003.

[4] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu "Mobile ADHOCnetworking: imperatives and challenges", School of Engineering, University of Texas at Dallas, Dallas, TX, USA, 2003.

[5] K. Ren, T. Lib, Z. Wanb, F. Baob, R. H. Dengb, and K. Kima, "Highly reliable trust establishment scheme in ADHOCnetworks," The International Journal of Computer and Telecommunications Networking, ElSEVIER,vol. 45, no. 6, pp. 687–699, 2004.

[6] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008.

[7] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009.

[8] K. Lakshmi, S.Manju Priya A.Jeevarathinam K.Rama, K. Thilagam," Modified AODV Protocol against Blackhole Attacks in MANET', International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.

[9] Sen, J.; Koilakonda, S.; Ukil, A.; , "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile ADHOCNetworks", Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on , vol., no., pp.338-343, 25-27 Jan. 2011.

[10] A. Shamir, "How to share a secret," Communication of the ACM, vol.22, pp. 612–613, 1979.

[11] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Mitigation of Black Hole Attacks for AODV Routing Protocol", Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.

[12] Subash Chandra Mandhata, Dr.Surya Narayan Patro, "A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks" International Journal of Computer & Communication Technology (IJCCT).

[13] Rahila Patel Nisarg Gandhewar, "Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network",2012 Fourth International Conference on Computational Intelligence and Communication Networks.

© 2021 The authors. This is an open access article under the CC-BY license.