I. J. Computer Network and Information Security, **2016, 4, 37-43**
Published Online April 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.04.05

Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography

Nitin Khanna
College of Engineering and Management, Kapurthala, Punjab, India
E-mail: nitinkhanna300@gmail.com

Abstract—MANET is a decentralized network that has no infrastructure and nodes can communicate with each other by multi-hoping the messages. Due to this nature of MANET, it is prone to many security attacks in which packet drop attacks are very common. Various packet drop attacks like Blackhole attacks, Grayhole attack, Co-operative Blackhole attack, etc are the attacks that become a bottleneck in efficient routing and security in MANET. Various mechanisms are devised in past but none of them prove to be effective against all types of packet drop attacks. In this paper, a mechanism is formulated that enhances the AODV routing protocol with Trueness Level and Cryptography for effectively counter all types of packet drop attacks by mitigating them through avoidance and elimination of source of attack after detection. This mechanism is powered by efficient use of Cryptography in its natural form. This work is compared with published work Extended Data Routing Information mechanism against various parameters like Packet Delivery Ratio, Normalized Control Load, Accuracy and Reliability in the same environment and parameters in MATLAB 2013a.

Index Terms—AODV (Ad-hoc On-demand Distance Vector) Routing Protocol, Trueness Level, Security, Cryptography, Blackhole Attack, Grayhole Attack.

I. Introduction

MANET stands for Mobile ad-hoc network in which nature of nodes is mobile and they can freely move in the region of network either in regular or irregular pattern. It is due to this ad-hoc nature, the routes are formed spontaneously as and when needed. Due to this nature, MANET is opened to various security threats like packet drop attacks, spoofing, etc. As there is no centralized system it is very difficult to maintain smooth communication in MANET and various mechanisms has been devised for mitigation of these attacks. For routing the traffic in MANET various routing protocols like AODV (Ad-hoc On-demand Distance Vector) routing protocol, DSDV (Destination Sequenced Distance Vector) routing protocol, DSR (Dynamic Source Routing) protocol, etc are used. These routing protocol can be classified as pro-active, re-active or hybrid depending upon route forming and maintenance mechanism. Pro-active routing protocol maintains all the routes all the time whether it is needed or not while re-active routing protocol formulates the path only when it is needed. Hybrid routing protocol is a mixture of this routing schemes.

Pro-active routing protocols provides all the routes ready to use as and when needed but it causes overhead due to the effort wasted in formation of those routes that will never be used. On the other hand, re-active routing protocols start the route discovery only when the route is needed and thus limits the overhead caused for maintaining routes all the time but initial effort is wasted to form the route when needed that causes delay in communication because of absence of route between two end parties that need to communicate. The choice of routing protocol affects the mechanism employed for security against various attacks and thus needs to be carefully chosen upfront.

Packet drop attacks like Blackhole, Grayhole and co-operative Blackhole are of the main concern while designing security and routing in MANET. Blackhole attack is an attack in which a malicious node act as a Blackhole node by replying to a RREQ packet send by a source node with a fake RREP packet and thus ensures the source that it has the most optimum route to the desired destination. But actually it does not have any route to that particular destination. When the source node sends data packets to that destination through the Blackhole node as intermediate node, the Blackhole node drops each and every data packet and thus hampers communication between two end nodes. This is the most basic and commonly occurred packet drop attack but its consequences are very hazardous if security measures are not taken. Many mechanisms are formulated that can detect Blackhole attack with ease but still it is a very serious and most common threat to the smooth routing in MANET.

Grayhole attack is a special type of Blackhole attack, in which malicious node selectively drop packets and thus it is very difficult to detect it using mechanism used for Blackhole detection. This packet drop attack is very severe as it is very difficult to design mechanism that accurately differentiates a malicious attack from an unwilling collusion that forms the basis of false positive. This attack is rather complex as it is driven by a artificial

Copyright © 2016 MECS

intelligence in the malicious node or continuous surveillance by an outside party for selection of packets to be dropped that fools the other fair nodes and does not come into notice if ordinary packet drop measures are taken.

On the other hand, Co-operative Blackhole attack is a special type of Blackhole attack in which two or more malicious nodes act in co-ordination to perform packet drop. One node acts as forwarding node that reply with fake RREP packet to RREQ packet sent by source. When source node sends the data packet through this malicious node, it forwards that packet to its co-operative partner in attack and that node performs the actual packet drop attack. Thus both the nodes acts together to perform packet drop attack without coming in notice to other nodes in the Network.

II. Related Works

In this section, some published works are reviewed that come from various authors that provides solutions for detecting and mitigating packet drop attacks [11] and provide security to the communicated information from passive attacks. Watchdog [7] and Pathrater [7] are the mechanisms that are widely used for detecting Blackhole attack. Watchdog is used to detect Blackhole nodes by using a counter. This counter is maintained by every node in the network and it is incremented by node only if it does not overhear the forwarding of packet by next hop to a particular destination. If the counter reaches a predefined threshold, the next hop is marked as Blackhole and source node is notified. But standard Watchdog is not much accurate due to false positives and true negatives. Pathrater [7] mechanism is used to avoid forming routes that includes Blackhole nodes. This mechanism uses a rating method between 0 and 1 and Blackhole nodes are given -100 rating that is minimum of all. The reliability of path is calculated from the average of path rating of the nodes involved in the formation of that path. Thus, if the path involves a malicious node then its path rating would be very low and no such path is considered by the node. A wide variation of standard Watchdog mechanism is formulated by different authors for more accurate Blackhole detection. Bayesian Watchdog [13] and Kalman Watchdog [5] uses filters that will help in minutely detect Blackhole and avoid false positives and true negatives. These mechanisms use complex equation for calculating the reliability and trust level of nodes and nodes are considered malicious only if they yield a result below threshold after calculation through complex filter equations. These variation leads to high network overhead as a lot of data is transferred between all the nodes in the MANET. Multilevel Threshold Secret Sharing [16] and repository scheme [3] are solutions to the passive attacks and secure the information flowing through the network by the use of cryptography and calligraphic techniques that hides data from unintended intermediate nodes. These techniques provide good data security but puts high amount of load on the processor of mobile nodes. These techniques lead to high security overhead as they requires complex calculations at both ends that takes a lot of processing time and energy. Collaborative Watchdog [4] is also used for precisely detecting Blackhole attack and disseminates this information to other nodes in the network. This mechanism is based on the co-operation of various nodes in the network that shares the information about their neighbouring node and helps in disseminating information about malicious nodes. In this collaborative Watchdog, if the attacks go undetected, this will prove more problematic than the standard Watchdog. Watchdog-AODV [17] is a fast mechanism which collaborate Watchdog and AODV routing protocol and improves the route discovery. This mechanism on discovery of the malicious node, mark that node as Blackhole [11] and notify the source about the detection of a malicious node and route discovery mechanism is quickly initiated by the source. It suffers from similar drawbacks as of standard Watchdog mechanism. EDRI table [18] used in Grayhole detection and mitigation as it holds the Gray nature of malicious node. It uses further request and further reply [18] message to acquire gray nature of nodes. But it will create lots of load on the storage and processing of nodes and creates network overhead as well for acquiring gray nature of neighbourhood malicious nodes. This work from theoretic point of view is good but neglects the most important issue of power consumption is MANET. In [3], cryptography is used to enhance security of the routing protocol that provides greatest reliability but the handling of cryptography is very inefficient that leads to more power dissipation of nodes which is critical in MANET. Enhanced W-AODV [15] that includes various new fields provides better security but do not detect co-operative attacks. Trueness Level [15] helps in forming reliable routes in a more efficient way and proves to be excellent in connection with modified AODV routing protocol. Trueness Level [15] provides a simple algorithm to generate a trust hierarchy and co-operation among fair nodes for malicious node detection and dissemination of such information.

III. Proposed Enhancement in AODV Routing Protocol

In this section, enhancement in the AODV Routing Protocol [10] is proposed and discussed. Two new fields are introduced in RREQ [10] packet and three new fields are added in RREP packet of AODV routing protocol. Two fields, DR bit and Trueness Level [15] are common in both RREQ and RREP packet while third additional field in RREP packet is Inceptor field. RREQ and RREP packets that are used in route discovery in AODV routing protocol with enhancement are shown as follow: -

Copyright © 2016 MECS

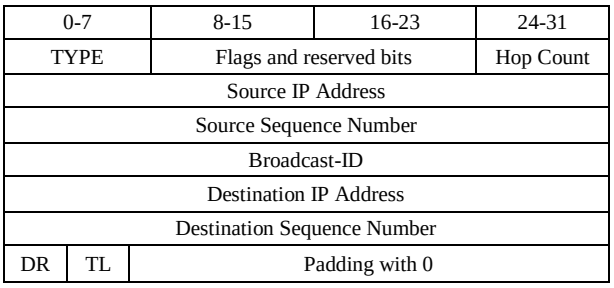

Fig.1. Modified RREQ Packet in Enhanced AODV

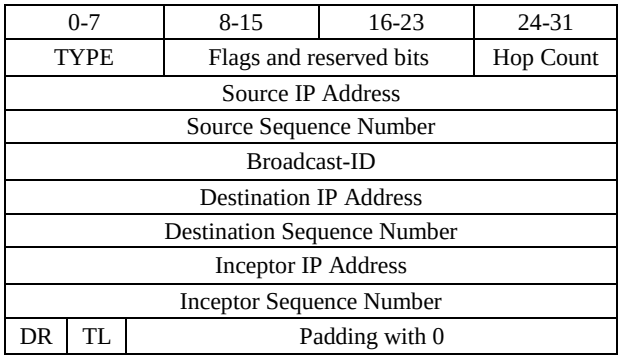

Fig.2. Modified RREP Packet in Enhanced AODV

A. DR Field

DR Field is a 1-bit field introduced in control packets to allow reception of only those RREP packets by source that is sent by the intended destination when DR bit is set to 1. When this bit is set to 0, in that case nodes take control packets as ordinary AODV control packets. With use of this field, we can ensure that the path formed between two nodes, i.e., source and destination is a reliable one. Thus it helps in avoidance of any form of packet drop attack as the paths formed under the enhanced AODV routing protocol are free from any type of malicious node.

This bit is set to 1 by source in RREQ packet, when source wants to communicate with the destination node for the first time or when the previously formed path is attacked by malicious node which is detected and eliminated and a new route discovery mechanism is started to form a new path of high reliability. With the help of this field, the route formed is of optimum quality and is highly reliable. But this will create some extra overhead in the network, so this bit needs to be used efficiently and effectively only when needed at extreme.

B. Trueness Level Field

Trueness Level [15] Field is a 3-bit field that depicts the Trueness Level of the path that is currently under consideration for formation. This mechanism helps in avoiding any type of packet drop attack once the network gets settled and all the nodes establish their identity as well as detecting and eliminating the malicious nodes that are acting as Grayhole [1]. Grayhole attack is detected through the lowering of Trueness Level to Level 0. This three bit field is used to show all the eight Trueness Levels from 0 to 7 as explained follow:-

Table 1. Bit Representation of Trueness Level Field

Field Code	Trueness Level	Order
000	Level 0	Lowest
001	Level 1	
010	Level 2	
011	Level 3	
100	Level 4	
101	Level 5	
110	Level 6	
111	Level 7	Highest

This field tells the current Trueness Level of path that the nodes are considering for formation between source and destination node. The value of this node keeps on updating at each node with the mechanism followed by Trueness Level in RREQ packet. Every node on reception of RREQ packet from its neighbour, updates the value of this field according to the algorithm followed by Trueness Level mechanism.

C. Inceptor Fields

Inceptor Fields include two subfields that tells the IP address and sequence number of node that originates the RREP packet in reply to the RREQ packet so that source knows the identity of the node that incepted the RREP packet to its query for path in the form of RREQ packet to a particular destination. With the help of this field, the source can take action against the culprit malicious node if the path leads to packet drop attack with ill-intentions. In that case the source node marks the inceptor node as malicious and notifies its neighbourhood about it with the use of Trueness Level mechanism.

D. Use of Cryptography

Cryptography provides the basis for security measures in this approach. Various techniques of cryptography and the way in which these techniques are used are explained as follow:-

Diffie-Hellman Algorithm for Symmetric key Generation

Diffie-Hellman algorithm [12] is used to generate symmetric key between two end nodes to ensure confidentiality of information that will be communicated through data packets. In our proposed mechanism when two nodes need to communicate for the very first time, the source node initiates Diffie-Hellman Algorithm [12] by sending parameters for calculation of symmetric shared key. Then destination after authentication through RSA Signature [12], continue the algorithm and generate a common secret shared key.

Additive Cipher for encryption/decryption process

Whenever a node needs to send data packets to a destination node, it uses additive cipher [12] to encrypt the message data using secret key which it has earlier exchanged and created along with the destination node using Diffie-Hellman algorithm. In additive cipher, a fixed number is added to the data for its encryption and the same number is subtracted for decryption at destination.

Copyright © 2016 MECS

Message Digest using MD5 algorithm

Message digest [12] is used to ensure the integrity of data packets that are transmitted from source node to the destination node. Although the integrity is somewhat ensured through the use of Watchdog mechanism but still there are some loop holes in that process so that is why Message Digest is used. So that if any discrepancy is found in received data that must not go undetected. For generating digest of the message MD5 algorithm [12] is used.

RSA Signature

RSA signature [14] algorithm plays a very important role in maintaining authentication, identification and security of attacks in MANET. First of all, RSA signature is used to ensure the security of secret key generation. It is used to sign Diffie-Hellman [12] parameter to ensure that the base of communication between two end nodes is secured. RSA signature will help in avoiding Blackhole nodes to generate fake RREP control packet when DR bit is set to 1. In that case, when DR bit is set to 1, the source will accept RREP packet that comes all the way from destination itself which is authenticated through RSA signature algorithm. If the secret key is already generated then the RREP control packet will include RSA signature on the digest of secret key or if it is the first communication then it must include RSA signature [14] on Diffie-Hellman [12] parameter. The third role of RSA signature is to help in ensuring authenticity of sender as the data sent by the source node is officially signed by the source through its private key and packet is accepted only after validation of signature through public key of sender node.

E. ACK Counter

This scheme is used to ensure that the data packet is delivered safe and sound to the destination and is accepted by it. It will not send an ACK packet if the destination does not receives a packet or discards the packet due to security issues. Every node while communicating with other nodes maintains an ACK counter for each node separately, which is incremented for each data packet sent and decremented for each verified Acknowledgement packet received and a threshold value is set for these counters which is same for all of them. If the counter reaches the threshold value then the malicious node that is performing packet drop attack is marked using Inceptor field data captured at the time of route establishment and new path is established once again.

IV. Simulation Environment

All the simulations and analysis of result is done in MATLAB 2013a. The proposed work has been compared with the published work Extended Data Routing Information (EDRI) [18] for various network evaluation parameters. All the source nodes send data packets of size 512 bytes that exclude the header of packet. Each packet includes encrypted data through secret key cryptography. The simulation is done in static environment. The assumed environment and parameters used for simulation of proposed work are described in the table below:-

Table 2. Simulation Environment and Parameters

PARAMETER	VALUE
NUMBER OF NODES	15,30,45,60
SPEED OF NODES (m/sec)	5,10,15,20
ANTENNA TYPE	OMNI-DIRECTIONAL
% OF BLACK HOLES	10%
% OF GRAY HOLES	10%
AREA	2000m X 2000m
NEIGHBOUR TIME	1s
PAUSE TIME	10s
NO. OF SCENARIOS	18
WIRELESS INTERFACE	802.11
ROUTING PROTOCOL	Enhanced AODV
% OF COLLABORATIVE BLACKHOLES	5%
TRANSMISSION RANGE	250m
ENVIRONMENT TYPE	STATIC
TRAFFIC MODEL	CBR
TRANSPORT PROTOCOL	TCP
MOBILITY MODEL	RANDOM WAY POINT

Various simulation scenarios are obtained by varying the node mobility speed, node density that is defined by number of nodes in the network and focus on detection of particular type of packet drop attack.

V. Result and Discussion

During the simulation experiment, the prosposed work has been evaluated against four paramaters, that are Packet Delivery Ratio, Normalized Control Load, Accuracy in detection of various packet drop attacks and Reliability of path formed and is compared with the published work Extended Data Routing Information (EDRI) [18] mechanism. After comparison, the result is discussed to enlighten the impact of our proposed mechanism in the form of enhancement in AODV routing protocol. The results are calculated by varying both node density and node mobility. The network parameters are compared in graphs with node mobility that is calculated by averaging the values of parameters at various node density, i.e., by changing number of nodes in the network and keeping node mobility constant at that time. The result on the basis of different network parameters are shown and discussed as follow: -

A. Packet Delivery Ratio (PDR) v/s Node Mobility

Packet Delivery Ratio is defined as a ratio of total number of packets received by intended destination and the total number of packets generated by the source node

for that particular intended destination. Higher the Packet Delivery Ratio, higher the effectiveness of network and it needs to be more than 4:5 at any node mobility speed and even in presence of attacking nodes for network to work for advantage to its user.

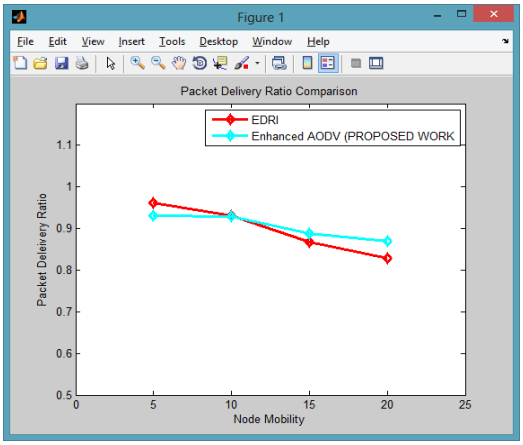

Fig.3. Packet Delivery Ratio Comparison

In the previous figure, through comparison we can easily see that with varying speed of node mobility, the Packet Delivery Ratio does not show drastic drop at higher mobility. That means, it remains stable over the varying mobility and is consistently touching 90% mark which is not the case in the EDRI [18] that shows high drop in PDR as compared to the proposed mechanism. The packet delivery ratio is on higher side in my proposed work as it provides mitigation against packet drop and form reliable paths that leads to better and accurate delivery of packets to its intended destination.

B. Normalized Control Load v/s Node Mobility

Normalized Control Load is defined as the ratio of total number of Control Packets generated by nodes in the network to the total number of Data Packets received and positively acknowledged by the intended destination node. Normalized Control Load needs to be in control and minimum even under high mobility and high node density. This network parameter decreases with increase in mobility due to breakage of paths between nodes due to unreachability.

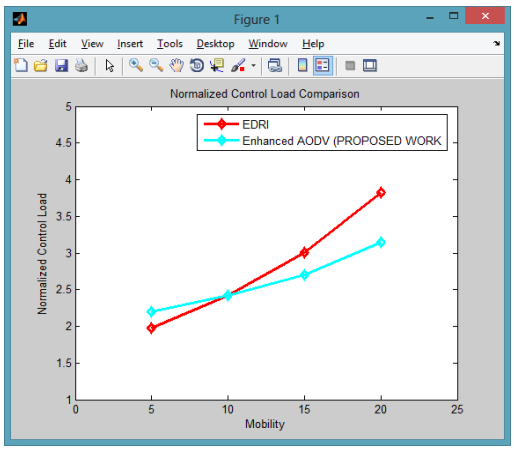

Fig.4. Normalized Control Load Comparison

From the above comparison, it is clear that proposed Enhancement in AODV routing protocol leads to lower control load on network as compared to EDRI mechanism and it shows steep increase even at higher level of node mobility. At lower node mobility, the control load is little on the higher side. This is due to fixed cryptographic overhead that can be overlooked from the security point of view. But as the mobility speed increases to more practical ones the proposed work meets the expectation and creates only a limited amount of control load including the cryptographic overheads.

C. Accuracy in Packet Drop Attack Detection v/s Node Mobility

Accuracy in detection of packet drop attack is calculated as the ratio total number of packet drop attacks detected by the mechanism to the total number of packet drop attacks actually occurred in the network. It is calculated in percentage so for that the result is multiplied with 100.

The mechanism needs to be highly accurate to be of good use in practical scenarios that are very hazardous to extremely cumbersome attacks.

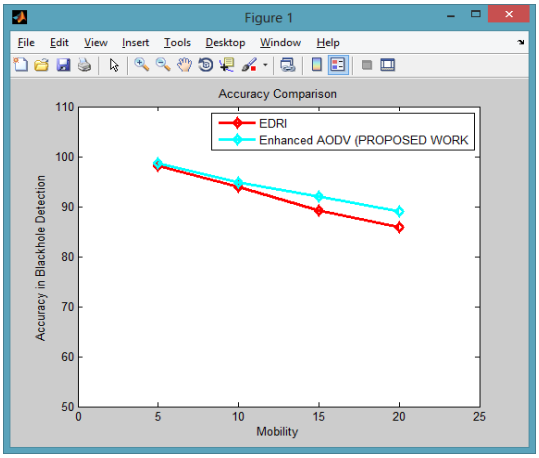

Fig.5. Accuracy in Packet Drop Attack Detection Comparison

From the above comparison, it is clear that our proposed mechanism shows higher level of accuracy even at high mobility among nodes and it shows steep decrease. DR Field helps in avoiding all forms of packet drop attacks and formation of more reliable paths. Trueness Level Field helps in forming reliable paths as well as collaborative approach to disseminate information about malicious nodes and Grayhole attack detection and elimination. Inceptor field helps in detecting both Blackhole and Co-operative Blackhole attacks. So, all these enhancement works in collaboration to detect and mitigate all forms of Packet Drop Attacks.

D. Reliability of formed Path v/s Node Mobility

Reliability of path formed in the network is measured as security of the path and its freedom from various packet drop attacks, misbehaving nodes and potential misbehaving nodes. It defines how reliable the path is in long run so that no packet dropping attack takes place in that path. Reliability is calculated as the ratio of total

Copyright © 2016 MECS

number of reliable and attack free path formed to the total number of actual path formed during the experiment. It is calculated in percentage.

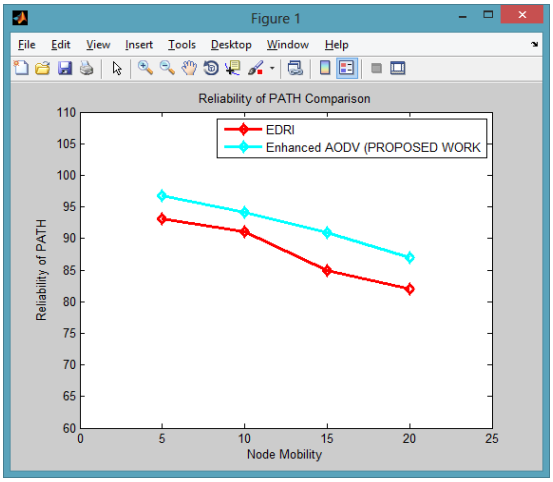

Fig.6. Reliability of Path Comparison

Path reliability decreases with the increase in node mobility again due to breakage of formed path due to unreachability and a narrow chance for malicious node to enter in the network for attack. Still however, the proposed mechanism continuous to form reliable path and shows steep lowering even at high mobility speed.

VI. Conclusions and Future Work

Packet drop attack is a very sensitive issue in MANET and it needs to be handled efficiently and effectively. The proposed mechanism, enhancement in AODV routing protocol and use of cryptography helps in identifying, avoiding, mitigating and eliminating all types of packet drop attack that too with greater accuracy and limited control load on the network. It increases the Packet Delivery Ratio that is apparent due to the fact that lesser number of undetected attacks led to more reliable paths that increases PDR. In addition to this, use of cryptography provides security to the data and that too at limited cryptographic overhead. So it can be said that this proposed mechanism provides better security with more reliable paths and better delivery of data packets without putting much load on the network.

As future work I propose enhancement in mechanism that decreases the constant overhead caused by the cryptography. In addition to that enhancement is proposed to detect a very active form of attack Wormhole Attack [1] that is also a type of co-operative attack leads to disruption of routing process.

References

[1] Punya Peethambaran and Dr. Jayasudha J. S., "SURVEY OF MANET MISBEHAVIOUR DETECTION APPROACHES", International Journal of Network Security & Its Applications, Vol.6, No. 3, May 2014.

[2] Gaurav, Naresh Sharma Himanshu Tyagi, "An Approach: False Node Detection Algorithm in Cluster Based MANET", International Journal of Advanced Research in Computer Science and Software Engineering Vol. 4, No. 2, February 2014.

[3] K. Sahadevaiah, Prasad Reddy P.V.G.D., "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks", MacroThink Institute, Vol. 3, No. 4, 2011.

[4] Enrique Hernández-Orallo, Manuel D. Serrat, Olmos Juan-Carlos, Cano Carlos, T Calafate, Pietro Manzoni, "A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs", Springer , August 2013.

[5] Tushar Sharma, Mayank Tiwari, Prateek kumar Sharma, Manish Swaroop, Pankaj Sharma, "An Improved Watchdog Intrusion Detection Systems In Manet", International Journal of Engineering Research & Technology, Vol. 2, No. 3, March 2013.

[6] Vrutik Shah, Nilesh Modi "An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks", International Journal of Computer Applications, Vol. 69, No.7, May 2013.

[7] D.Anitha, Dr.M.Punithavalli "A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS", IJCSMC, Vol. 2, No. 3, pp. 112 – 119, March 2013.

[8] Carlos de Morais cordeiro and Dharma P. Aggarwal, "Mobile Ad-hoc Networking", 2004.

[9] Andreas Tonnesen "Mobile Ad-hoc Networks", 2004.

[10] Charles E Perkins Elizabeth M Royer "Ad hoc On Demand Distance Vector Routing", 1999.

[11] Rashid Hafeez Khokhar Md Asri Ngadi Satria Mandala "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", 2008.

[12] Behrouz A Forouzan "Data Communications and Networking 4th Edition", Tata McGraw Hill Companies, 2004.

[13] Serrat-Olmos, M.D. Hernandez-Orallo, E. ; Cano, J., Calafate, C.T., Manzoni, P., "Accurate detection of black holes in MANETs using collaborative bayesian watchdogs", Wireless Days(WD), IEEE Conference, pp. 1-6, Nov. 2012.

[14] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 vol. 2, pp. 120–126, 2013.

[15] Nitin Khanna, Parminder Singh, "Mitigating Blackhole and Security attacks in MANET using Enhanced W-AODV with Trueness Level and Cryptography", IJRECE, vol. 3, no. 2, pp. 146-151, 2015.

[16] Lein Harn Miao Fuyou, "Multilevel threshold secret sharing based on the Chinese Remainder Theorem", Information Processing Letters 114, ELSEVIER, pp. 504–509, 2014.

[17] Tarun Varshney, Tushar Sharmaa, Pankaj Sharma (2014), "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network", IEEE International Conference on Communication Systems and Network Technologies, pp. 217-221, June, 2014.

[18] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal,"Detection and Removal of Co-operative Blackhole and Grayhole attacks in MANET", International Conference on System Engineering and Technology, Bandung, Indonesia, September, 2012.

Copyright © 2016 MECS

Authors' Profiles

Nitin Khanna, born in 1991, has done his Masters in Computer Science & Engineering in 2015 and currently working as Assistant Professor, Department of Computer Science & Engineering at College of Engineering & Management, Kapurthala, Punjab, India.In recent years, He has worked in the field of ad-hoc networks and work towards solution to the secure and reliable communication in MANET and mitigation of various attacks in MANET.

How to cite this paper: Nitin Khanna,"Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.4, pp.37-43, 2016.DOI: 10.5815/ijcnis.2016.04.05

Copyright © 2016 MECS