Preventing Black Hole Attack in AODV Routing Protocol using Periodic Trust Handshake Based Malicious Behavior Detection Mechanism

Bhawna Singla[1,#], A. K. Verma[2], L. R. Raheja[3]

[1]*Professor. CSED, Panipat Institute of Engineering and Tech.*

[2]*Professor, CSED, Thapar University*

[3]*Professor, IIT Kharagpur*

[#]Corresponding Author, Email: *bhawna_singla@yahoo.com*

***Abstract* - Detection of black hole is a challenging task. Further, isolating such malicious nodes from communication is also a great challenge. Several previous works addresses trust based model for detection and prevention of malicious nodes. Trust based models will consume time to study the neighbor transmissions and will try to identify trustable nodes based on their data forwarding behavior. But this approach will need considerable quantity of time to identify malicious nodes by constantly monitoring the traffic of the neighbor nodes. Another drawback of existing model is, false positives – that is, the standard trust based detection mechanisms may wrongly mark a trustable node as non-trustable node if that node, by chance, is not participating in communication even without any bad intention. To avoid false positives, and to improve the detection accuracy, in this work, we propose the use of a Periodic Trust Handshake mechanism. Our Periodic Trust Handshake based detection mechanism will detect the malicious nodes very quickly in a short time military rescue like MANET scenario without much increase in overhead. To prove its better working, we simulated a MANET short time communication scenario and measured the performance of standard AODV with and without black hole attack and compared it with our Periodic Trust Handshake based Trust AODV (PTH-AODV) protocol in terms of different metrics. The proposed PTH-AODV will use a Periodic Trust Handshake mechanism for the reliable detection of malicious behavior in MANET.**

***Keyword*: AODV, Trust, Periodic Trust handshake model, Performance Metric**

1. INTRODUCTION

Mobile Adhoc Network (MANETs) [1][2] means collection of network utilized for communication where the nodes keeps on moving and thereby changing its topology. The nodes also act as a router because they also participate in forwarding the packet from source node to destination node through number of intermediate nodes. These routing decisions constitute to become a routing protocol.

In MANETS, basically there are two types of routing protocol i) Passive Routing protocol ii) Active Routing Protocol depending on the route determination. If the route is determined in advance then it is known as passive routing protocol e.g. destination sequenced distance vector routing protocol(DSDV), Wireless Routing Protocol(WRP) etc. [3]. If the route is determined after the request of route then it is known as active routing protocol e.g. AODV[4]. In frequently changing environments active routing protocol is preferred over passive routing protocol. Adhoc On Demand Distance Vector Routing Protocol (AODV) is chosen for study in this paper.

However due to number of factors such as use of IP addresses, participation of intermediate node in decision making etc. AODV Routing Protocol is encountered by number of attacks[9][10]. One such attack is Blackhole attack. In case of Black hole attack, the intermediate node claims itself as having the shortest route through itself. Once the malicious node is chosen as the intermediate node, it drops all or some of the packets (control or data). Due to loss of packet, network performance degrades significantly.

2. Blackhole Attack

In AODV, whenever there is a route requirement, source node initiates a route discovery process , as shown in figure 1.Source node broadcasts a route request packet (RREQ) to its neighbor as shown in figure . The purpose of RREQ message is to determine the destination node or to find the intermediate node that has route to the destination node. Whenever such a node is found, it immediately responds by sending back the Route Reply message called RREP. Due to Black hole attack, the malicious node intends to have the shortest path through itself and once the path is chosen it drops all the packets that pass through that path. There are two methods two cause Black hole attack 1) RREQ 2)RREP according to the control packet on which malicious action took place. Fig.2 shows the working of AODV protocol in presence of blackhole attack.

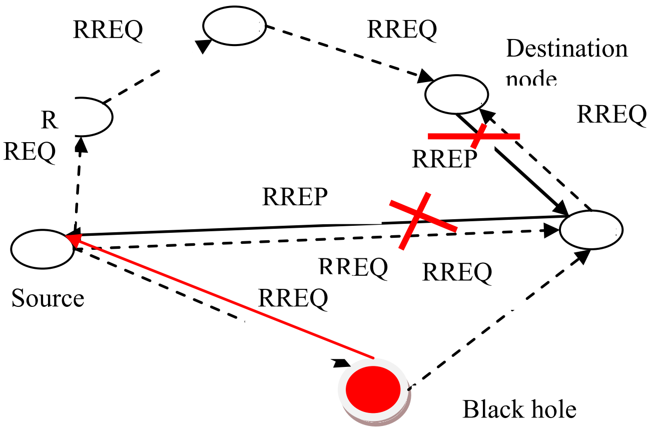


Fig 1: Working of AODV in presence of black hole

3. Previous works on black hole attack detection

Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao [5] presented the detailed survey of blackhole attack. In this paper, different detection schemes[6-17] of blackhole attack are presented in chronological order and further compared with each other.

Jin-Hee Cho et. al. in “A Survey on Trust Management for Mobile Ad Hoc Networks”[18] presented detailed definition of trust. One such definition is relationships among the entities that participate in the protocol. The main properties of trust can be summarized as below

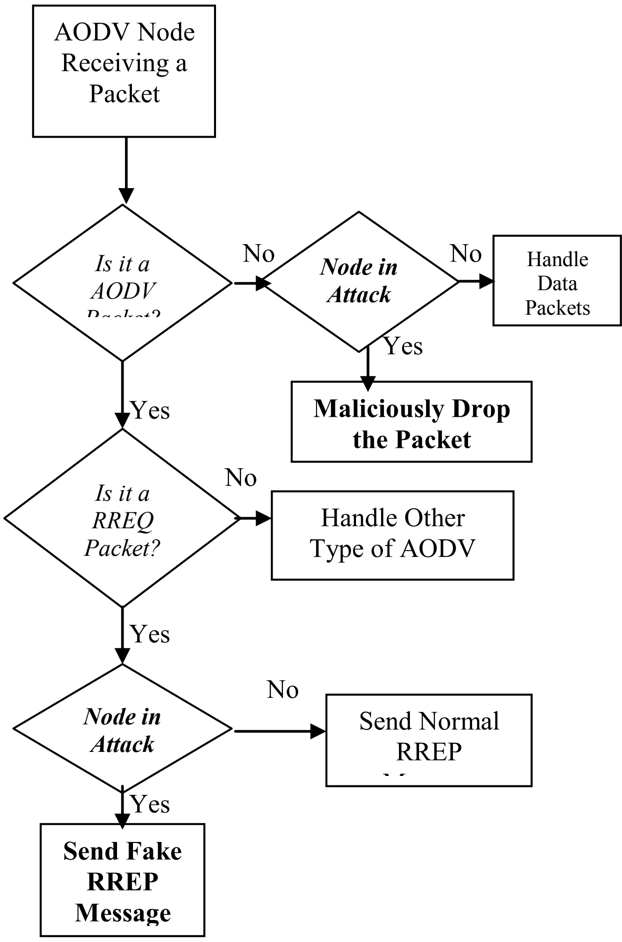


Fig 2: Flow chart of AODV working

.

1. Dynamic: Due to mobility of node, this information is highly changing.
2. Subjective: A node can have different levels of trust for the another node as nodes have highly dynamic topology.
3. Non-Transitive: If A Trust B and B trust C then it does not necessarily mean that A trust C
4. Asymmetric: If A trust B then it does not necessarily mean B trust A.
5. Context Dependent: The trust relationship is highly context dependent.

Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung, and Dusit Niyato in “A Survey of Trust and Reputation Management Systems in Wireless

Communications "[19] summarized the trust management schemes that have been developed for MANETs as below

1. Secure routing protocol: Security is added to routing protocol using cryptographic protocols. Examples include ARAN, ARIADNE, SAODV, SAR , SRP etc. Further, security may be added by identifying selfish and malicious node.
2. Authentication: MANETs works on the IP addresses as the source node sends the request packet destined for the IP address of destination node. So, a more security is required to determine the node claiming a IP address is actually that node. The Protocols like Verma *et al*. (2001) [20], Pirzada & McDonald (2004) [21], Ngai & Lyu (2004) [22]
3. Intrusion detection: Intrusion detection system is a software of hardware tool that helps in automatically helps in detecting intrusions in the MANETs[23,24,25]. Since the topology is highly dynamic, therefore the detection process is distributed among number of nodes.
4. Access control: This part is restricted in determining whether or not to grant the access to resources.
5. Key management: While using the cryptographic algorithms, this part is used to maintain the security of public and private keys.
6. Trust and reputation management system: Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung, and Dusit Niyato in "A Survey of Trust and Reputation Management Systems in Wireless Communications " [26]states that cryptographic measures often helps in achieving data confidentiality, integrity, authentication and access control. However, it may not prevent node from misbehaving maliciously in the network. Asad Amir Pirzada, Chris McDonald, and Amitava Datta in Performance Comparison of Trust-Based Reactive Routing Protocols [27] splits the process in the three parts i) trust derivation ii) computation and iii) application.
   a. Trust derivation: Whenever a source node sends a packet (data or control), it sets its receiver into promiscuous mode to overhear the intermediate node. The sending node checks the integrity field of the packet. If there is no change then it means the node has forwarded the packet in benevolent manner and therefore direct trust counter in incremented by one otherwise it is decremented.
   b. Trust Computation: The Trust value[27] is computed using Situational Trust $Txy(n)$.
   c. Trust Application: The application of trust value differentiates the node into two categories: benevolent and malevolent. In case of AODV, when the source node initiates the RREQ message for the destination then it does not searches for the shortest path rather it searches for path with the highest trust value.

4. About the proposed work

A malicious mode such as black hole node will constantly drop most of the packets that it receives and will not genuinely participate in route discovery process. Especially, the black hole nodes will not send or forward anything.

The trust based on the packet forwarding behavior of neighbor can be used for detecting misbehavior as we generally expected. This model has been previously presented in several literatures[28-30]. But, by the same trust based logic, some of the neighbors those who were silent and not actively participated in communications will get wrongly identified as malicious. So, simple trust based models will mark lot of non malicious nodes as malicious nodes. This will initiate lot of link failures. That is, the link between sources to destination will get broken at different locations on their path because of this false identification of malicious nodes.

The Periodic Trust Handshake based trust AODV (PTH-AODV) proposed in this paper will overcome that problem and reduce the possibility of such false marking of non malicious nodes as malicious nodes. A simple Periodic Trust Handshake mechanism will help to prevent such false identification.

The main advantage of the proposed detection and prevention scheme is : it will detect and prevent the malicious nodes in the very early stage of AODV route discovery process. So, it will not need any manipulation in routing tables in the route resolving process, because, by the design, it will avoid including malicious hops in routing table even at the route discovery process itself.

5. Implementation of The Proposed Malicious Behavior Detection in AODV

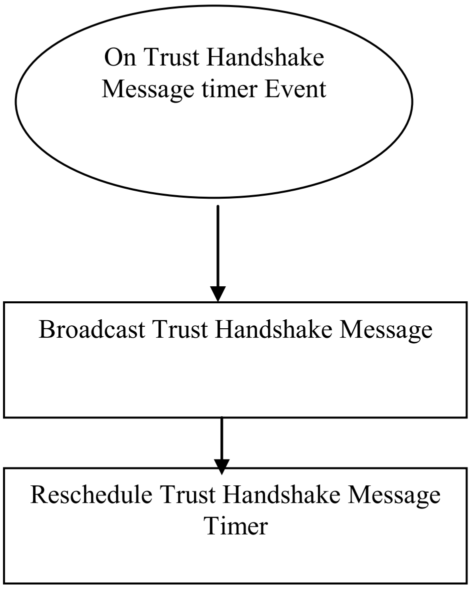
Implementation of Periodic Trust Handshake Mechanism: Generally, a trust factor based on the packet forwarding behavior of neighbor can be used for detecting misbehavior as previously presented in several literatures. For example, a trust factor of a node can be derived based on the number of forwarded packets at that neighboring node. But, by the same trust based detection logic, some of the neighbors those who were silent and not actively participated in communications will get low trust factor and will be wrongly identified as malicious. Because of this, the link between source to destination will get broken at different locations on their path because of this false identification of malicious nodes.

In our proposed Periodic Trust Handshakebased trust AODV (PTH-AODV), it will overcome that problem and reduce the possibility of such false marking of non malicious nodes as malicious nodes by introducing a Periodic Trust Handshake mechanism.

In this model, the nodes will send a "trust handshake" in a periodic fashion. The frequency of this "trust handshake" message will be controlled by a variable max_TrtustHandshake_Interval. This Periodic Trust Handshake mechanism ensures that handshake packet in a periodic fashion so that the neighbor trust factors will be updated with respect to the mobility of the node.

The following flow diagram explains the implementation of Periodic Trust Handshake Mechanism in AODV routing agent.

Fig 3 : The Periodic Trust Handshake Message Handler


On Trust Handshake Message timer Event
Broadcast Trust Handshake Message
Reschedule Trust Handshake Message Timer

The Functions Modified for Attack Detection and Prevention.

The function TrustHandshakeTimer(): The Periodic Trust Handshake Mechanism is implemented with the help of a new timer function in AODV.

The function AODV:: SendTrustHandshakePacket(): This function will generate a Trust Handshake packet and transmit it with respect to the conditions explained in the figure 3

*The function AODV::recvAODV():*In this function, the trust based detection of malicious behavior has been implemented. As shown in the figure 4 of previous section the malicious behavior detection is done based on the trust factor of the previous hop node from which the message was received.

6. Results And Discussion

We used network simulator version NS2.35 under Ubuntu linux operating system for obtaining this results. We have implemented the black hole attack as well as attack detection and prevention mechanism on the aodv code of NS2 and did the simulation with the parameters presented in this section and evaluated the performance with respect to the metrics discussed in this section.

The Simulation Parameters

Common Parameters

In our simulation, we used following as mentioned in table I common parameters while setting up the network.

Table I: Common parameters used in network

Topographical Area	**1800 X 500**
Mobility	***2*0m/s**
Pause Time	***2*0s**
Total SimulationTime	***1*00s**
Routing Protocol	**AODV**
MobilityModol	**RandomWaypoint**
Channel Model	**WirelessChannel**
Propagation Model	**TwoRayGround**
PhyModel	**WirelessPhy**
MacModel	***8*02_11**
AntennaModel	**OmniAntenna**
Queue	**DropTail-PriQueue**
Queue length	**50**

Traffic Parameters:

The following parameters in table II are used to setting up the tcp flows with some periodic data.

Table II : Traffic parameters

Transport Agent	**TCP**
No Flows	**10**
Traffic Type	**CBR**
Packet Size	**1Kb**
Interval	**100ms**
Rate	**10kb**

The following parameters in table III are used to setting up the udp flows with some periodic data.

Table III: Traffic parameters related to UDP flows

Transport Agent	**UDP**
No Flows	**10**
Traffic Type	**CBR**
Packet Size	**1Kb**
Interval	**100ms**
Rate	**10kb**

Variable Parameters

The following parameters in table IV are used as variables for analyzing the impact of the attack and detection on different condition.

Table :IV Malicious data used in analysis

Malicious Nodes	**15**
Total Nodes	**40, 50,60**
AODV with	**No Attack, Black Hole Attack, PTH Attack Detection**

Here we see the analytic results of comparision of black hole attacks with normal AODV (it means performance without any attack). And it is studied with Respect to Different Network Size. In the following analysis the total number of nodes in the network is varied as 40, 50 and 60 and among them, the number of malicious nodes kept as 15 and the impact is measured using different metrics.

The following figure shows the impact of attack and detection and prevention mechanism in terms of total data packets sent at application source. As shown in the figure 4, under the presence of Blackhole Attack the application source itself can not able to send much. But while detection the proposed PTH-AODV was able to send as much as normal AODV without any attack.

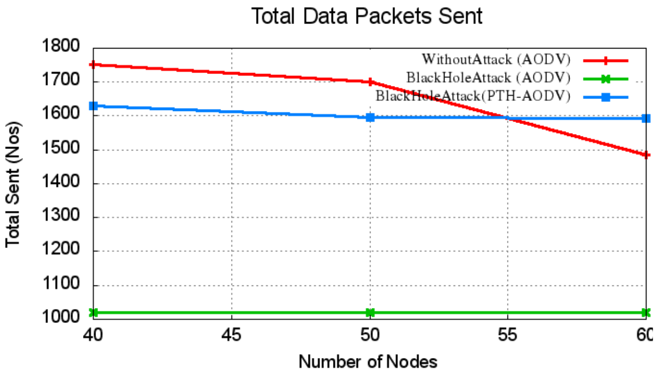


Fig 4: Network Size vs Sent Packets

The following figure 5 shows the impact of attack and detection and prevention mechanism in terms of total data packets received at application destination. As shown in the figure, under the presence of Blackhole Attack the application destination itself can not able to receive anything. But while detection the proposed PTH-AODV was able to receive as much as normal AODV without any attack.

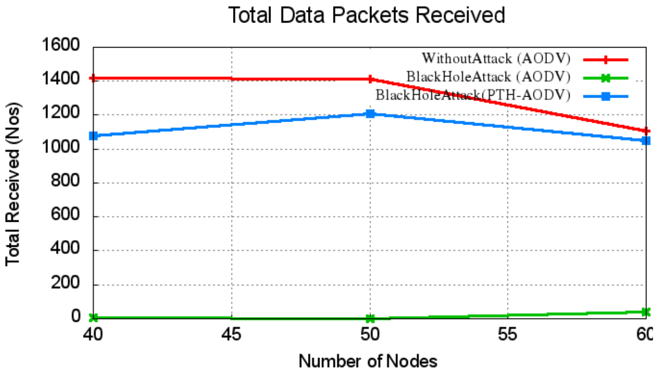


Fig 5: Network Size vs Received Packets

The following figure 6 shows the impact of attack and detection and prevention mechanism in terms of routing load. As shown in the figure, under the presence of Blackhole the routing load is very high. But with proposed PTH-AODV based detection and prevention mechanism, the routing load was almost equal to that of normal AODV.

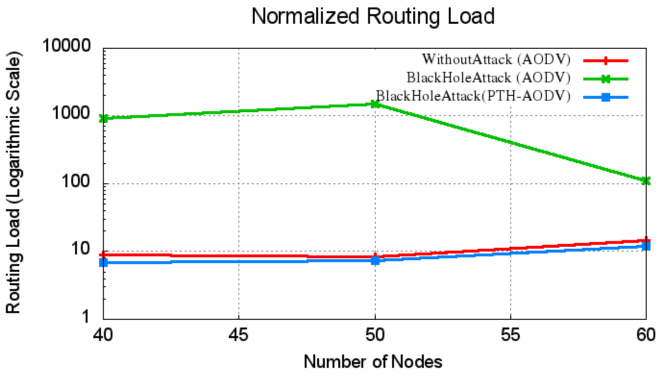


Fig 6: Network Size vs Routing Load

The following figure 7 shows the impact of attack and detection and prevention mechanism in terms of MAC load. As shown in the figure, under the presence of Blackhole the MAC load is very high. But with proposed PTH-AODV based detection and prevention mechanism, the MAC load was almost equal to that of normal AODV.

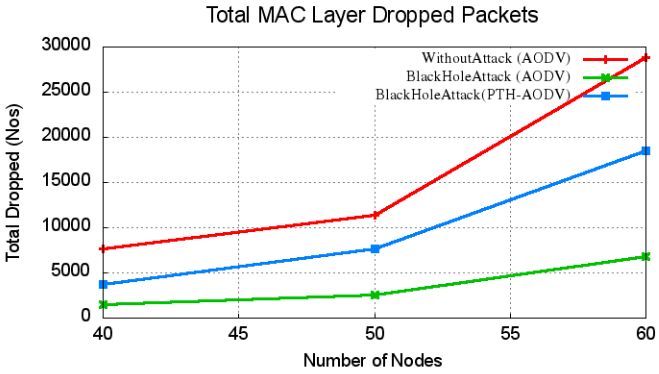


Fig 7: Network Size vs MAC Load

The following figure 8 shows the impact of attack and detection and prevention mechanism in terms of total dropped packets at application layer. As shown in the figure, under the presence of Blackhole Attack the lot of packets were dropped at application layer. But while detection, the packet dropping of proposed PTH-AODV was very much reduced and al most equal to that of normal AODV without any attack.

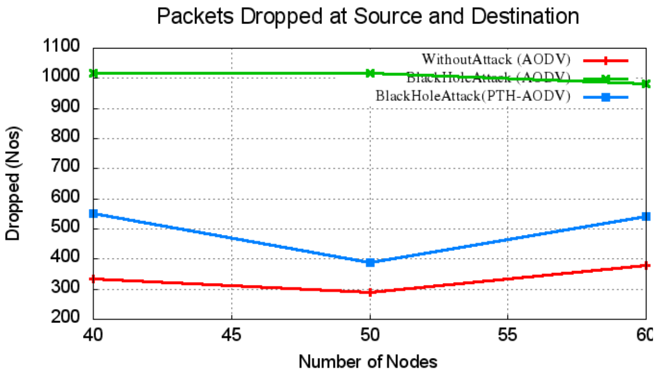


Fig 8: Network Size vs Packets Dropped At Application Layer

The following figure 9 the impact of attack and detection and prevention mechanism in terms of throughput. As shown in the figure, under the presence of Blackhole Attack the throughput was almost equal to zero. But with detection, the throughput of proposed PTH-AODV was very much improved and almost equal to that of normal AODV without any attack.

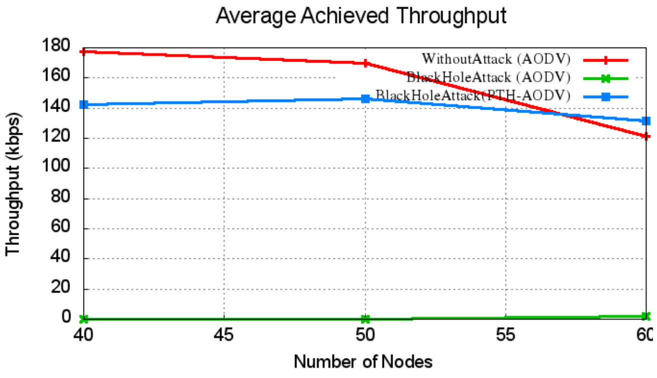


Fig 9: Network Size vs Throughput

The following figure 10 shows the impact of attack and detection and prevention mechanism in terms of PDF. As shown in the figure, under the presence of Blackhole Attack the PDF was almost equal to zero. And at low network density PDF is equal to zero. For example, at 40 nodes, it is zero because, among the 40 nodes, 15 are malicious- so that they will able to break all the communication between other nodes. But with detection, the PDF of proposed PTH-AODV was very much improved and almost equal to that of normal AODV without any attack.

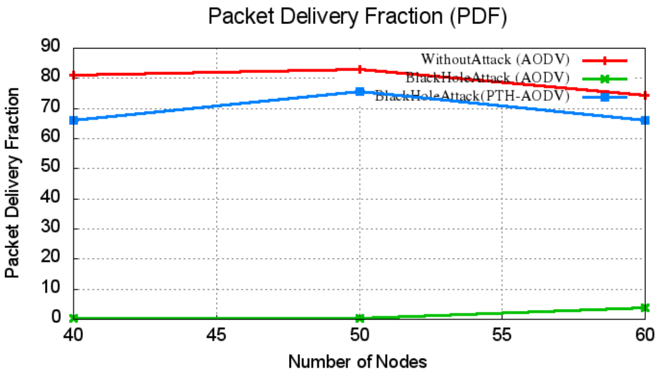


Fig 10: Network Size vs PDF

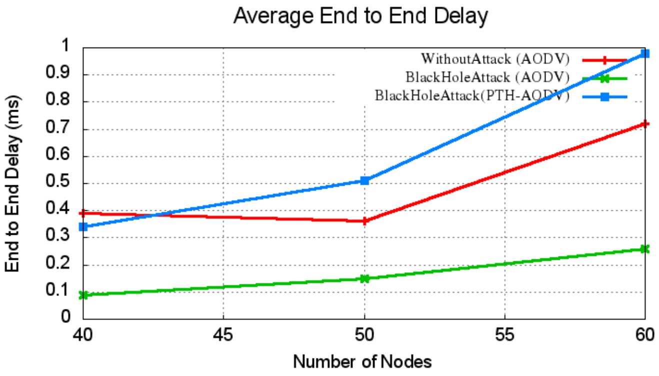


Fig 11 Network Size vs End to End Delay

The EED of PTH-AODV was little bit higher than normal AODV. Because, under attack detection and prevention, alternate route will be resolved by avoiding malicious nodes on a path, So that the path length will get increased and hence will increase the end to end delay as shown in figure 11.

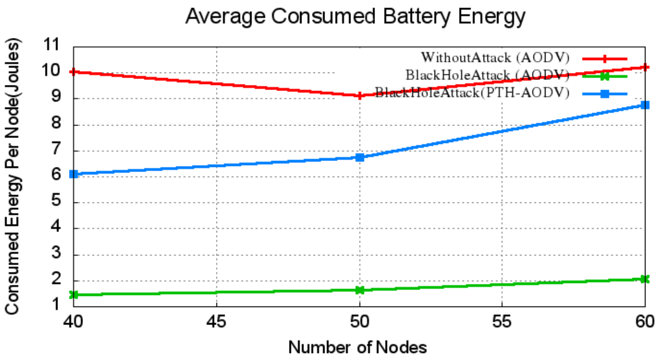


Fig 12: Network Size vs Battery Energy

The energy consumption in the case of proposed PTH-AODV is little bit lesser than normal AODV as ahown in figure12. This obviously proves the better working of proposed detection model.

The following figure 13 shows the impact of attack and detection and prevention mechanism in terms of overhead. As shown in the figure, under the presence of Blackhole the overhead is minimum – because, the black holes just break all the communication. But with proposed PTH-AODV based detection and prevention mechanism, the overhead becomes equal to that of normal AODV – it signifies that the proposed PTH-AODV works almost equal to normal AODV..

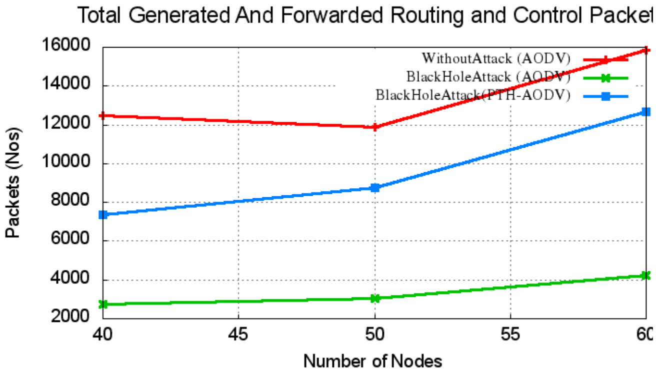


Fig 13: Network Size vs Overhead

The following figure 14 shows the impact of attack and detection and prevention mechanism in terms of total maliciously dropped packets at MAC layer. For the first look, one may think as this as a wrong result because of the decrease in malicious dropping in the case of attack as well as detection and prevention (PTH-AODV). But it is not. The dropping in the case of black hole attack is decreased because, the malicious packet dropping is only happening at routing layer. The dropping in the case of attack is less than all because, PTH-AODV little bit higher than attack without detection because, PTH-AODV will try to avoid black holes so that, initiate new route discovery process and this causes more packet generation and loss at MAC layer.

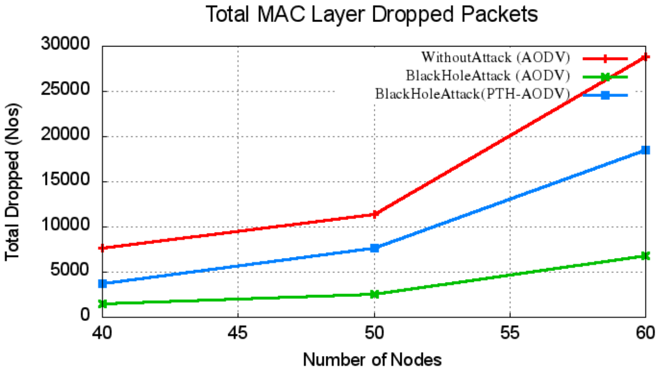


Fig 14: Network Size vs MAC Layer Dropped

The following figure 15 shows the impact of attack and detection and prevention mechanism in terms of total maliciously dropped packets at network layer. For the first look, one may think as this as a wrong result because of the increase in malicious dropping in the case of detection and prevention (PTH-AODV). But it is not. The malicious dropping in the case of PTH-AODV is increase because; it is trying to send the packet in one way or another by avoiding malicious nodes. The retransmissions involved in this process increases malicious packet dropping.

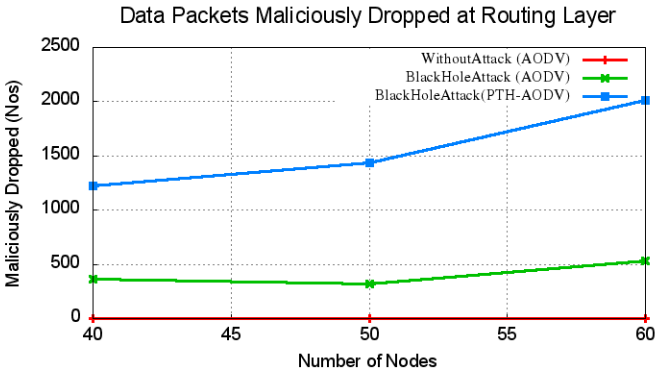


Fig 15: Network Size vs Malicious Drops at Routing Layer

7. CONCLUSION

In this work we proposed a periodic trust handshake based detection of black hole attack. We implemented out PTH-AODV under ns2 and compared its performance with the results of Standard AODV and Standard AODV under attack. The main advantage of the proposed PTH-AODV is : it will detect and prevent the malicious nodes in the very early stage of route discovery process. So, it will not need any manipulation in routing tables in the route resolving process, because, by the design, it will avoid including malicious hops in routing table of normal nodes at the route discovery process itself.

We did lot of simulation and analysis and arrived at significant and interpretable results. We measured the impact of the attack as well as the detection and prevention mechanism with suitable metrics and explained the improvements in performance. According to the arrived results, our proposed periodic trust handshake based malicious node detection and prevention mechanism works good and successfully detected black hole nodes in the network and avoided establishing routes though them. As shown in the results of the previous section, the proposed PTH-AODV improved the throughput and pdf almost equal to that of Normal AODV.

In this work, we used unencrypted trust handshake messages in the design. But in future works, we may explore the possibility of using a private key/public key based encryption mechanism for more secure operation. It may increase the operational overhead, so that one may address issues related with overhead due to encryption based trust handshake mechanism.

References

[1] Akbani, Rehan, Turgay Korkmaz, and G. V. S. Raju. "Mobile ad-hoc networks security." Recent Advances in Computer Science and Information Engineering. Springer Berlin Heidelberg, 2012. 659-666.

[2] Conti, Marco, and Silvia Giordano. "Mobile ad hoc networking: milestones, challenges, and new research directions." IEEE Communications Magazine 52.1 (2014): 85-96.

[3] Masoudifar, Mina. "A review and performance comparison of QoS multicast routing protocols for MANETs." Ad Hoc Networks 7.6 (2009): 1150-1155.

[4] Karthikeyan, B., N. Kanimozhi, and S. Hari Ganesh. "Analysis of Reactive AODV Routing Protocol for MANET." Computing and Communication Technologies (WCCCT), 2014 World Congress on. IEEE, 2014.

[5] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 1.

[6] Bar, Radha Krishna, Jyotsna Kumar Mandal, and Moirangthem Marjit Singh. "QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack." Procedia Technology 10 (2013): 530-537.

[7] Lo, Nai-Wei, and Fang-Ling Liu. "A secure routing protocol to prevent cooperative black hole attack in MANET." Intelligent Technologies and Engineering Systems. Springer New York, 2013. 59-65.

[8] Choudhury, Debarati Roy, Leena Ragha, and Nilesh Marathe. "Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole Attack." Procedia Computer Science 45 (2015): 564-570.

[9] Sun B, Guan Y, Chen J, Pooch UW (2003) Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[10] Al-Shurman M, Yoo S-M, Park S (2004) Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004

[11] Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009

[12] Raj PN, Swadas PB (2009) DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET.International Journal of Computer Science 2:54–59. doi: abs/0909.2371.

[13] Jaisankar N, Saravanan R, Swamy KD (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in

Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010.

[14] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) Improving AODV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010

[15] Su M-Y (2011) Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 34(1):107–117. doi:10.1016/j.comcom.2010.08.007

[16] Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009

[17] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L (2011) Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011

[18] Cho, Jin-Hee, Ananthram Swami, and Ray Chen. "A survey on trust management for mobile ad hoc networks." IEEE Communications Surveys & Tutorials 13.4 (2011): 562-583.

[19] Yu, Han, et al. "A survey of trust and reputation management systems in wireless communications." Proceedings of the IEEE 98.10 (2010): 1755-1772.

[20] R. R. S. Verma, D. O'Mahony and H. Tewari, "NTM – Progressive Trust Negotiation in Ad Hoc Networks," Proc. 1st Joint IEI/IEE Symposium on Telecommunications Systems Research, Dublin, Ireland, 27 Nov. 2001.

[21] A. A. Pirzada, C. McDonald, and A. Datta, "Performance Comparison of Trust-based Reactive Routing Protocols," IEEE Trans. Mobile Comput., vol. 5, no. 6, June 2006, pp. 695-710.

[22] E. C. H. Ngai and M. R. Lyu, "Trust and Clustering-based Authentication Services in Mobile Ad Hoc Networks," Proc. 24th Int'l Conf. on Distributed Computing Systems Workshops, 23-24 March 2004, pp. 582-587.

[23] Mohammed, Noman, et al. "Mechanism design-based secure leader election model for intrusion detection in MANET." IEEE transactions on dependable and secure computing 8.1 (2011): 89-103.

[24] Feiertag, Richard, et al. "Intrusion detection inter-component adaptive negotiation." Computer Networks 34.4 (2000): 605-621.

[25] Wang, Wenkai, et al. "Attack-proof collaborative spectrum sensing in cognitive radio networks." Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on. IEEE, 2009.

[26] Pirzada, Asad Amir, Chris McDonald, and Amitava Datta. "Performance comparison of trust-based reactive routing protocols." IEEE transactions on Mobile computing 5.6 (2006): 695-710.

[27] Govindan, Kannan, and Prasant Mohapatra. "Trust computations and trust dynamics in mobile adhoc networks: a survey." IEEE Communications Surveys & Tutorials 14.2 (2012): 279-298.

[28] Mohanapriya, M., and Ilango Krishnamurthi. "Modified DSR protocol for detection and removal of selective black hole attack in MANET." Computers & Electrical Engineering 40.2 (2014): 530-538.

[29] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." Proceedings of the 42nd annual Southeast regional conference. ACM, 2004.

[30] Sen, Jaydip, Sripad Koilakonda, and Arijit Ukil. "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks." 2011 Second International Conference on Intelligent Systems, Modelling and Simulation. IEEE, 2011.