ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com
Journal DOI: 10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Prevention for Black hole attack in MANET using AODV Protocol: Review.

Amrita Parashar, Vivek Parashar.
Amity School of Engineering & Technology.
Amity University, Madhya Pradesh.

Manuscript Info

Manuscript History:

Received: 15 February 2016
Final Accepted: 26 March 2016
Published Online: April 2016

Key words:

Corresponding Author

Amrita Parashar.

Abstract

Black hole attack is one of the active DoS attacks possible in MANETs so has got lots of attention by the researchers. Research focus mainly given to securing existing routing protocols, developing new secure routing protocols, and intrusion detection techniques. Researchers have proposed various techniques to prevent black hole attack in mobile ad-hoc networks. Many studies on MANET focus on the protocols used their security issues such as data encryption, authentication, trust, and cooperation among nodes, attacks on the protocols and proposed solutions or preventions.

Literature Survey:-

Buchegger and Le Boudec present the CONFIDANT protocol. Each node monitor the behavior of its next hop neighbors in a similar manner to watchdog. The information is given to the reputation system that updates the rate of the nodes. Based on the rating, the trust manager makes decisions about providing or accepting route information, accepting a node as part of a route and so on. When a neighbor is suspicious in misbehaving, a node informs its friends by sending them an ALARM message. If a node's rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. This does not address partial packet dropping.

Michiardi and Molva proposes the CORE scheme and various related issues in. In this scheme, every node computes a reputation value for every neighbor, based on observations that are collected in the same way as watchdog. The reputation mechanism differs between subjective reputation, indirect reputation, and functional reputation. Subjective reputation is calculated directly from neighbors past and present observations, giving more relevance to past observations in order to minimize false detection influence. Indirect reputation is the information collected through interaction and information exchange with other nodes using positive values only. Functional reputation is the global reputation value associated with every node. By avoiding the spread of negative rating, the mechanism resists attacks, such as denial of service. When a neighbor reputation falls below a predefined value, the service provided to the misbehaving node is suspended. The working of the model and its performance were not reported.

Banal and Baker propose OCEAN, a scheme for robust packet-forwarding. OCEAN, similarly to previous schemes, is based on nodes' observations. In contrast to previous mechanisms, no rating is exchanged and every node relies on its own information, so the trust management is avoided. The rating is based on a counter that counts the positive and the negative steps a node performs and based on a faulty threshold, the node is added to a faulty list. In the method for route selection, a DSR node appends an avoid list to every generated RREQ and a RREP based on this list. A second-chance mechanism is provided to give nodes that were previously considered misbehaving another opportunity to operate. OCEAN simulations concludes that a scheme which relays only on first-hand observation performs almost as well and sometimes even better than a scheme that also relies on second-hand information. OCEAN also fails to deal with the misbehaving nodes properly.

Bracha Hod, in his thesis highlights various aspects of cooperation enforcement and reliability, when AODV is the underlying protocol. Furthermore, it presents a scalable protocol that combines a reputation system with AODV that addresses reputation fading, second-chance, robustness against liars and load balancing. The proposed solution constructs different reputation properties and misbehaving reaction better suiting to AODV. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it want to intercept. The proposed approach to combat the Black hole attack is base on node's activity as example number of sent RREQ, number of sent RREP, number of received data and number of sent data packets. When an intermediate node reply RREQ packet, the voting process initiated about activity of replier.

H.Weerasinghe and H. Fu introduces the use of DRI (Data Routing Information) to keep track of past routing experience among mobile nodes in the network and crosschecking of RREP messages from intermediate nodes by source nodes. The main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table. It is evident that maintaining past routing experiences wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication.The second drawback is over consumption of limited bandwidth.

H. Deng, W. Li and D. Agrawal, research is similar to Weerasinghe's technique except an additional weakness of inability to prevent attack from multiple black hole nodes.

P. Raj and P. Swadas , proposed an adequate solution by checking RREP messages from intermediate nodes for possible intrusion activities. This technique is successful based on the assumption of cooperation between nodes. If a mobile node discovers a possible attack by an intruder, the discovering node notifies all other nodes the presence of an attack by broadcasting an ALARM message. This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast. Generate a token, which is appended to the data packets to identify the authenticity of the routing packets and to choose correct route for data packets. TRP provides significant reduction in energy consumption and routing packet delay by using hash algorithm.

Balakrishnan *et al*. propose a mechanism to defend against flooding and packet drop attacks in MANETs. They present an obligation-based model called fellowship and describe how this model can be used to identify and penalize malicious and selfish nodes.

Zhang and Lee proposes a distributed and cooperative intrusion detection model based on statistical anomaly detection techniques. In the intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and confirmation message, the source determines the validity of path according to its policy.

Huang et al use both specification-based and statistical-based approaches. They construct an Extended Finite State Automation (EFSA) according to the specification of AODV routing protocol and model normal state and detect attacks with anomaly detection and specification-based detection. An approach based on dynamic training method in which the training data is updated at regular time intervals has been proposed.

Marti et al. proposes two techniques that improve throughput in an ad hoc network in the present of misbehaved nodes .The watchdog method is used for each node to detect misbehaving nodes in the network.
When a node sends a packet to next hop, it tries to overhear the packet forwarded by next hop. If it hears that the packet is forwarded by next hop and the packet matches the previous packet that it has sent itself, it considers the next hop behaves well. Otherwise it considers the next hop misbehaves .The path rater uses the knowledge about misbehaving nodes acquired from watchdog to pick the route that is most likely to be reliable. Each node maintains a trust rating for every other node. When watchdog detects a node is misbehaving, the trust rating of the node is updated in negative way. When a node wants to choose a safe route to send packets, path rater calculates a path metric by averaging the node ratings in the path .Marti et al implemented the solutions on DSR protocol using ns2 as simulation environment. The simulation result shows the throughput of the network could be increased by up to 27% in a network where packet drop attack happens. However routing overhead is also increased by up to 24% protocol.

In a black hole attack, several malicious nodes falsely claim a new route to the destination in order to absorb all packets coming from the source. To combat this kind of routing protocol attack, Hongmei et al. proposed a solution that revolved around waiting and checking the replies from all other neighboring nodes and then deciding on the safe route.

Juwad and Al-Raweshidy presents an experimental performance comparison between Secure-AODV (SAODV) and AODV. They claim that there has been a lack of performance and security analysis in real network test-beds. A quantitative performance comparison between routing protocols AODV and SAODV is presented in an experimental test-bed and using the OPNET network simulator. These results show that SAODV is more effective in preventing two types of attacks (control message tampering and data dropping attacks) than AODV.

Chen et al. quantitatively evaluate an approach detailing network survivability in wireless adhoc networks. They define network survivability as a combination of network failure impacts and failure durations and use a performance metric called excess packet loss due to failures.

Ariadne has proposed ad-hoc routing protocol that provides security in MANET and relies on efficient symmetric cryptography. This protocol is based on the basic operation of the DSR protocol. In [9], a secure routing protocol based on DSDV has been proposed. Hash chains have been used to authenticate hop counts and sequence numbers.

ARAN uses cryptographic public-key certificates in order to achieve the security goals. The goal of SAR is to characterize and explicitly represent the trust values and trust relationships associated with ad-hoc nodes and use these values to make routing decisions.

Secure AODV (SAODV) is a security extension of AODV protocol, based on public key cryptography. Hash chains are used in this protocol to authenticate the hop count. Adaptive SAODV (A-SAODV) has proposed a mechanism based on SAODV for improving the performance of SAODV. In a bit of modification has been applied to A-SAODV for increasing its performance.

TRP employs hash chain algorithm to generate a token, which is appended to the data packets to identify the authenticity of the routing packets and to choose correct route for data packets. TRP provides significant reduction in energy consumption and routing packet delay by using hash algorithm.

In Robust Routing by Lee, Han, Shin, the intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and authentication message, the source verifies the legitimacy of path according to its policy. With the view to secure routing in MANET several intelligible researches has been carried out. Hu, and Johnson proposed SEAD, a secure routing protocol based on DSDV that employs Hash chains to authenticate hop counts and sequence numbers

Researchers have proposed solutions to identify and eliminate a single black hole node. Misbehavior detection and reaction are described in, by Marti, Giuli, Lai and Baker. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. However, according to simulations, it is highly effective in source routing protocols, such as DSR. The path rater uses the knowledge from the watchdog to choose a path that is most likely to deliver packets. The path rating is calculated by averaging the rating of the nodes in the path, where each node maintains a rating for all the nodes it knows in the network. Watchdog is used intensively in many solutions for the cooperation problem. The main drawback of this idea is that it enables selfishness and misbehaving nodes to transmit packets without punishing them, and thus encourages misbehavior.

Lennart Conrad developed an improved trust-based routing DSR. With the trust-based routing DSR each node keeps the trust value of all other nodes .Different from most reputation solutions which uses passive acknowledgement to detect whether neighboring node has forwarded a packet or not, trust-based DSR uses an explicit acknowledgement packet sent by the receiver to confirm that the packet has been forwarded by all the nodes along the route successfully. If the sender receives the acknowledgement packet within a timeout, it will increase the trust values of all the nodes along the route. Otherwise it will decrease the trust values. Then a node will choose a most trustful route when it has to send a packet. The main contribution of Lennart's solution is that he proposed alternative trust

value updating and route selection strategies. The simulation results show significant improvement in throughput compared to regular DSR.

Conclusion:-

Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET, security of MANET is one of the important features for its deployment. In our thesis work we study black hole attack and proposed a feasible solution to prevent single black hole attack on the AODV routing protocol. The proposed solution is evaluated by the performance metrics - end-to-end delay, network load and Throughput. In our study we analyzed three different scenarios with the above stated performance metrics. We also compare our proposed solution results with the previous work done solution results .The throughput of our proposed solution is more as compared to previous solutions results. The delay and network load is also less than the previous work done results.

Reference:-

1. Yibeltal Fantahun Alem, Zhao Cheng Xuan "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" 2010 2nd International Conference on Future Computer and Communication.V3-672
2. Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach" International Journal of Engineering Science and Technology (IJEST). ISSN: 0975-5462 Vol. 3 No. 4 Apr 2011
3. Razan Al-Ani, "Simulation and Performance Analysis Evaluation for Variant MANET Routing Protocols" International Journal of Advancements in Computing Technology, Volume 3, Number 1, February 2011
4. Shree Om, Mohammad Talib ,"Wireless Ad-hoc Network under Black-hole Attack" International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 628-633
5. Abderrahmane Baadache, Ali Belmehdi, " Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks" International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010
6. Shervin Ehrampoosh, Ali Khayatzadeh Mahani,"Secure Routing Protocols: Affections on MANETs Performance" 1st International conference on communication engineering
7. IRSHAD ULLAH, SHOAIB UR REHMAN,"Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols" School of Computing Blekinge Institute of Technology, Sweden
8. Thodeti Srikanth, Dr.V.B.Narsimha, "Simulation-based approach to performance study of routing protocols in MANETs and ad-hoc Networks" International Journal of Computer Science and Network Security, VOL.11 No.9, September 2011
9. Abdalla Ahmed Fekry Mahmoud," Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN)" The American University in Cairo School of Sciences and Engineering
10. OPNET Tutorial http://www.ensc.sfu.ca/research/cnl School of Engineering Science Simon Fraser University
11. Cong Hoan Vu, Adeyinka Soneye, "An Analysis of Collaborative Attacks on Mobile Ad hoc networks" School of Computing Blekinge Institute of Technology Soft Center SE – 37225 RONNEBY SWEDEN
12. Bracha Hod ,"Cooperative and Reliable Packet-Forwarding On Top of AODV" School of Engineering and Computer Science, the Hebrew University of Jerusalem Israel
13. Karan Singh, R. S. Yadav, Ranvijay ,"A REVIEW PAPER ON AD HOC NETWORK SECURITY" International Journal of Computer Science and Security, Volume (1): Issue (1) 52
14. Jinhua Guo, Weidong Xiang, and Shengquan Wang, "Reinforce Networking Theory with OPNET Simulation" Journal of Information Technology Education Volume 6, 2007
15. James D. Boggs, "A Tutorial on Basic Use of OPNET IT Guru®, Academic Edition"
16. Anipakala Suresh, "Performance Analysis of Ad hoc On-demand
17. Distance Vector routing (AODV) using OPNET Simulator" Communication Networks, University of Bremen
18. Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy ," AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes" International Journal of Advanced Computer Science and Applications, Vol. 2, No. 8, 2011
19. H. A. Esmaili , M. R. Khalili Shoja , Hossein gharaee, " Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator" World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 2, 49-52, 2011 49
20. Saud Rugeish Alotaibi,"Stability of Secure Routing Protocol in Ad hoc wireless Network" De Montfort University United Kingdom, England 2010
21. Roman Dunaytsev, "OPNET Overview and Examples" Tampere University of Technology, November 30, 2010

22. Opnet Technologies, Inc. “Opnet Simulator,” Internet: www.opnet.com,
23. Mehdi Medadian, Ahmad Mebadi, Elham Shahri,“ Combat with Black Hole Attack in AODV Routing Protocol” Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15 -17 December 2009 Kuala Lumpur Malaysia
24. Xiaohua Chen, Qiu Zhong, Danpu Liu “An Improved MAODV Protocol Based on Mobility Prediction and Self-pruning Flooding ” 2009 International Conference on Communications and Mobile Computing