International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25409-25415

http://www.ripublication.com

Novel Approach To Avoid Black-Hole By Applying Trust Based Method In Manet

T. Senthil Murugan
Associate Professor, Department of CSE,
Vel Tech University, Avadi, Chennai - 600062
C. Ambika Bhuvaneswari
Assistant Professor, Department of ECE,
Vel Tech University, Avadi, Chennai - 600062
M. Thanjaivadivel
Assistant Professor, Department of CSE,
Vel Tech University, Avadi, Chennai – 600062
D. Sugumaran
Assistant Professor, Department of IT,
Vel Tech University, Avadi, Chennai – 600062

Abstract

Preserving the confidentiality of the adhoc networks are most important factor to maintain the stability of the network. There are numerous numbers of protocols are available to perform the work but the unfortunate turnout of those protocols will be partial coverage or fail to cover the nodes, packets etc. The major problems faced by MANET are worm-hole, black-hole, Sybil, and route table alteration etc. Particularly black-hole attacks are the most hazardous because of its self proclaiming activity of calling itself as a safe method to find the minimal routing path and makes the traffic pull to its side. Resulting in the total damage to the data occurs. In this paper we discuss about black-hole attack and proposing technique to avoid the same. Also we are going to discuss few of related works to acquire knowledge about black-hole attack and we propose an effective and efficient solution to solve and avoid the black hole issues occur in the network. The proposed solution will going to be a novel proposition device specific method where the base trust is created along the nodes of the network and the clusters will decide the malforming node based on the trust created.

Keywords: MANET, Black hole Attack, Trust Based Method

Introduction

The mobility and seamless connectivity makes MANET the most preferred network across in many real time tasks. So, the protocols involves in deciding the route search between source and destination. The topological management will be carried out by the existing protocols. The nature of the network is dynamically designed that makes the network to allow the neighbors to connect or disconnect the network at any point of time. The attacks are mostly accompanied along with the protocol. The black-hole attacks are the most widely used attack to destroy the total network, Hence, the need for analyzing this attack most important at this point of time.

The hazardous nature of the black-hole attracts the traffic towards it by disguising itself as the best route to travel between the source and destination. This creates a serious gap in the security of the network causing the total damage to the network by pulling out the real data, that may be a important when the military data involved. Apart from the data loss there may other issues like low ratio in packet delivery and huge delay in data transfer. The proposed solution speaks about the configuration of the new node that will produce a much secure and safe environment by utilizing server-cluster-client model. Where a cluster is responsible to search the destination in shortest path, a server will take care of traffic monitoring and the client will be responsible for contacting the source-destination and neighbors.

The major goal is to find the finest solution to find and avert the black-hole. The various protocols are considered and studied to know their working style and the issues occurring at various stages, similarly the various techniques based on security are studied to find and give an idea about usage of the best possible technique inside the network. Later on the implementation of the proposed scheme that proposes a novel defense configuration and the topology for the network.

Literature Survey

The MANETs are prone to several attacks, most type of attacks are against physical layer, network layer, Mac layer. The basic mechanism of routing will be taken place in the above layers. They are two sort of network layer attacks, they are messages will not get forwarded and some changes in routing table. Basically, an attack can stop sending the messages to the neighbor.

Whenever an attacker selecting a route, its stop the entire relay. Usually, the black hole attack will be in dormant state until its neighbor initiates a request (RREQ). If a node receives the relay request then its replies with a false relay reply (RREP) with a unbelievable set of numbers. It makes the source to believe there is a fresh route available. Whenever it happens, the source ignores RREP from the neighbor and it will initialize transaction to the attacker. Now, the attacker takes the entire request and not sends the packet back. The black hole generally consumes all objects.

N.Raj et al. proposed a new method to avoid the black-hole by communicate the situation to the neighbor. Usually in AODV whenever the RREP sent to a node the receiving node will check for the sequential order of the route table. if the sequential order is more than the routing table then it will be accepted [2] but in this propose paper there has been a accumulation of checking the RREP sequential order is more

than the entry value. If the sequential order is higher than the then it will be considers the attackers

Here, an alarm will be raised to the neighbor whenever the attack occurs. The attacker has not updates in terms of the route table or the transaction not occurs to the other node. The entry value is updated by collection of data at the interval dynamically and it should be a typical value of the difference between the destination sequential order of the times lot across the sequential order in the route table.

There major advantage of this solution, the source places the major role by announcing the black-hole to the neighbor. Hence it can be avoided. Due to this, the Packet delivery ratio has improved by 30% when compared to the AODV.

Yang su et al. introduced a technique to separates and avoids the attackers. This technique introduces anti black-hole where it calculates the mistrustful value. The calculation has done on the mistrustful values of RREQ, RREP from node to node. If the neighbor is considered as a attacker then the whole route will be changed from the attack route. Whenever the mistrustful value of the node goes over the entry value, a stop message sent to the neighbors. As a result, the attacker will be completely frozen from the other nodes. The major disadvantage of this technique is it will stay only with in a particular region. This may not be helpful in all cases. Therefore, we need a special technique to establish a truncation between two nodes.

yang su et al. proposed a good technique by using honeypot members that will efficiently uses the network topology and find the mistrustful routing calls. They will be employed as the travelling agent that will roam the entire network and imitate the attacker by transacting similar request. Every honeypot will contain a log on the possible attacker as the safety precaution. The major drawback is it will not be helpful for the MANET because it executes lots of traffic and has know back boned authority.

Designing Network

The proposed solution will be based mainly on efficient configuration of the network and avoiding the black-hole. This section will explain about various models that might be used in the system.

The major step towards the effective attack analysis is through configuration of the nodes which is responsible to maintain the integrity of network and effective part of communication.

a. Group Header Node

The main purpose of the group header or the cluster head is to provide service to the requesting node. The traffic flow may occur inside the networks through the group header. Moreover, it is also necessary to find the next neighbor node or the final node and also to generate the secure key which is used to identify the child under the group header. It holds the liable in avoiding and finding the attacker node.

b. Configuring Main Node

The information about the entire network is stored in the main node. It includes the packet delivering ration, ids of the next node etc also it provides authentication to the

new neighbor node to join the network. The nodes cannot join without the authentication.

c. Configuring the End-User Node

The main work of the end-user node will be initiating the transaction to the neighbor node to perform communication. The communication will be initiated only when the neighbor will gets authentication from the main node under the same group header node.

Proposed Work

(i) Trust Based Model

The trust based model access the confidence value for the neighbors which are participated in the network. The confidence value is been assessed by performing the overall value across the network from the very best node. The confidence value varies from 1 to 10 where 1 will be the best worthy and 10 will be the unreliable. The entry value ranges from the minimum of 0.5 that makes uniformity across the network.

(ii) Group Header Algorithm

Consider N nodes and G group nodes in the network for initiate the transaction. The network has to works based on the following algorithm.

Step [1] Identify the group headers (GH) and its generates a key for authentication

Step [2] Flooding the key over the network under the cluster head

Step [3] Find the Source and Destination, If both are in similar group, do the following

i. Source sends data's to GH
ii. Check packet delivery ratio and key value of source node
iii. If it is wrong then labeled as malicious node and stop the packets.
iv. Else GH forwards the packets to destination

Step [4] Check if both source and destination are in various groups, do the following

i. Source sends data's to GH
ii. Check packet delivery ratio and key value of source node
iii. If it is wrong then labeled as wicked node and stop the packets.
iv. Otherwise, forward the data packets to concern group head then it will send to particular destination

In this algorithm, the source plays the major role by announcing the black-hole to the neighbor. Hence, it can be avoided and defended. This algorithm supports all region and a honeypot is created to maintain all the information on the attackers, it provides us a information vault to send data on the attacker to the neighbors.

Results and Discussion

The simulation has carried out over in an controlled environment with the help of Network Simulator (version 2.34) and evaluated the performance of the proposed algorithm. The simulation parameters are given in the following table.

Environment	Values
Simulation Area	1500 x 1500 m^2
No. of nodes	≈ 50 to 500
Simulation Time	10000 ms
Routing Protocol	AODV
Traffic Type	CBR
No. of Packets	≈ 100 to 1000
Bandwidth	2 Mbps

The Fig.1 is representing end-to-end delay of proposed algorithm and Adhoc on demand distance vector (AODV) routing technique. Both the protocol algorithms are performed at the time of attacks occurs. This results are clearly shown, the proposed method is better than AODV.

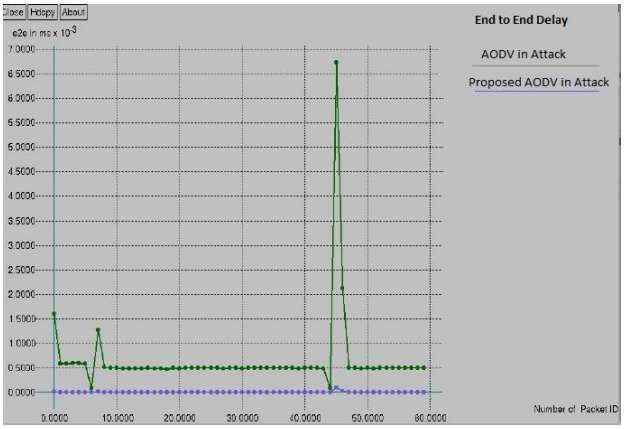

Figure 1: End to End delay when attack happens

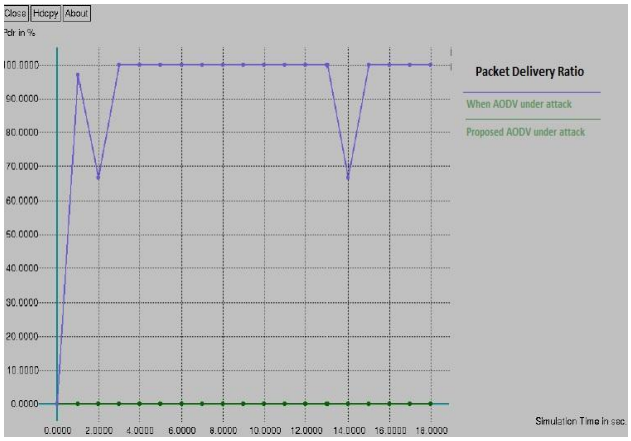

Figure 2: Packet delivery ratio when attack happens

The Fig. 2 has shown the packet delivery ratio (PDR) comparison between proposed method and AODV. Here, the proposed method has not affected the PDR even if attacks occur. Hence, our proposed method is better in point of improving the quality.

Conclusion

This paper explains about the detailed study over the previously proposed protocols, their advantages and disadvantages. Moreover the comparative study details about present AODV and the proposed algorithm. The major issue of MANET is its non-centralized environment that happens to be highly prone to the malignant attacks. Hence, to curb the black hole attack, we are setting up the topological network where a main node will take care of the node activities and the group header node will be responsible for the entire topological network. The proposed solution will provide the expected result with most accurate values in curbing the attacks happens inside the network. As a result oriented analysis this work will provide a environmental security of the network by setting up an network organizational structure.

References

[1] S.Djahel ; F. Nait-abdesselam ; Zonghua Zhang, " Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", IEEE Communications Surveys & Tutorials, Volume: 13 , Issue: 4, Page(s): 658 – 672, Year: 2011.

[2] I.Aad; J.-P Hubaux ; E.W. Knightly, " Impact of Denial of Service Attacks on Ad Hoc Networks," IEEE/ACM Transactions on Networking, Volume: 16 , Issue: 4, Page(s): 791 - 802, Year: 2008.

[3] S.Umang ; B.V.R Reddy ; M.N.Hoda, "Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using

minimal energy consumption," IET Communications, Volume: 4 , Issue: 17 Page(s): 2084 - 2094 Year: 2010.

[4] X. Li ; Z.Jia ; P.Zhang ; R.Zhang ; H.Wang, " Trust-based on-demand multipath routing in mobile ad hoc networks," IET Information Security, Volume: 4 , Issue: 4, Page(s): 212 – 232, Year: 2010.

[5] Hongmei Deng ; W.Li ; D.P.Agrawal, "Routing security in wireless ad hoc networks ," IEEE Communications Magazine, Volume: 40 , Issue: 10, Page(s): 70 – 75, Year: 2002.

[6] Ahmed, M. ; Hussain, M.A., "Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks," 2014 International Conference on Electronics, Communication and Instrumentation (ICECI), Page(s): 1 – 4, Year: 2014.

[7] Bo Yang ; Yamamoto, R. ; Tanaka, Y.Historical evidence based trust management strategy against black hole attacks in MANET 2012 14th International Conference on Advanced Communication Technology (ICACT), Page(s): 394 – 399, Year: 2012.

[8] Athmani, S. ; Boubiche, D.E. ; Bilami, A. "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," 2013 World Congress on Computer and Information Technology (WCCIT), Page(s): 1 – 5, Year: 2013.

[9] Osathanunkul, K. ; Ning Zhang, "A countermeasure to black hole attacks in mobile ad hoc networks," 2011 IEEE International Conference on Networking, Sensing and Control (ICNSC), Page(s): 508 – 513, Year: 2011.