Volume 6, Issue 9, September 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Hybrid Routing Algorithim Against Black Hole Attacks in MANETs

Zumer Jan
M.Tech CSE, Department of CSE
SDDIET, Panchkula, Haryana,
India

Nidhi Sharma
Asstt. Proff & HOD, Department of CSE
SDDIET, Panchkula, Haryana,
India

Abstract— ***In this work we are making a hybrid protocol of the reactive and proactive routing protocol protection of black hole attack for avoidance of attacks. This work is enhance the base work by implementing the future work described in which the protection of black hole attack is done using the hybrid of on demand and table based routing. The ideas are to detection the malicious node on the bases of trust value which calculated using the acceptances of the node.***

Keywords— ***MANET, Routing, AODV, DSR, ZRP***

I. INTRODUCTION

Wireless Ad-Hoc Network

A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad-hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

Wireless mobile ad-hoc networks are self-configuring, dynamic networks in which nodes are freely moving. In contrast to conventional power aware algorithms, EPAR identifies the capacity of a node not just by its residual battery power, but also by the expected energy spent in reliably forwarding data packets over a specific link [1]. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks “on the fly” - anywhere, anytime.

A wireless ad-hoc network, also known as IBSS - Independent Basic Service Set, is a computer network in which the communication links are wireless. The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to older network technologies in which some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts.

The earliest wireless ad-hoc networks were called “packet radio” networks, and were sponsored by Defense Advanced Research Projects Agency (DARPA) in the early 1970s. Bolt, Beranek and Newman Technologies (BBN) and SRI International designed, built, and experimented with these earliest systems. Experimenters included Jerry Burchfield, Robert Kahn, and Ray Tomlinson of later TEN-EXtended (TENEX), Internet and email fame. Similar experiments took place in the Ham radio community. It is interesting to note that these early packet radio systems predated the Internet, and indeed were part of the motivation of the original Internet Protocol suite. Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. Another third wave of academic activity started in the mid-1990s with the advent of inexpensive 802.11 radio cards for personal computers. The absence of infrastructure and its dynamic, diverse principal characteristics has made it more popular as well as vibrant because of it the Internet Engineering Task Force (IETF) is established in [2].Current wireless ad-hoc networks are designed primarily for military utility.

The decentralized nature of wireless ad-hoc networks makes them suitable for a variety of applications where central nodes can’t be relied on and may improve the scalability of networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Minimal configuration and quick deployment make ad-hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad- hoc networks to be formed quickly.

II. PREVIOUS WORK

[1] The black hole attack in wireless Ad Hoc network is major issue that needs efficient solutions. In blackhole attack more than one node can be malicious. Most of the time black hole attack occurs in large Ad Hoc

networks. The black hole attacks in wireless Ad Hoc network creates misunderstanding in network by introducing error in routing information that leads the node to select wrong path hence data lose occur. We have proposed a novel architecture of FRIMM (A Forced Routing Information Modification Model) prevents black hole attacks in wireless Ad-Hoc network by introducing automatic error correction in routing information that leads the node to select correct path thus secure transmission will take place between source and destination. In this model we assume that the network is centralized. In this model we have used the popular protocol AODV (Ad Hoc On-Demand Distance Vector).

[2] A wireless sensor network consists of geologically distributed autonomous sensors to monitor and control over physical or environmental conditions, like temperature, sound, pressure etc. And this information is passed through sensors in the network to a next location. Military applications was required the development of security in wireless sensor networks. Today such networks are used in many areas like industrial, health, and commercial applications. Black hole attack occurs when an intermediary captures and re-programs a set of nodes in the network to block/drop the packets and generates false messages instead of forwarding correct/true information towards the base station in wireless sensor network. Nearby many techniques have been proposed in the literature for detection and prevention of black hole attack in sensor network.

[3] Mobile ad hoc networks (MANET) are acquiring popularity today, as it offers wireless connectivity to the users irrespective of their geographical position. An ad-hoc network does not have a centralized infrastructure. It is a wireless network where nodes communicate with each other through multiple hops. If the nodes in the ad-hoc network change their positions dynamically, it is called a mobile ad-hoc network (MANET). It has characteristics like shared physical medium, autonomous terminal, limited physical security, infrastructure less communication, Dynamic topology, large degree of freedom, self organizing capability. Such characteristics provide an open environment for users to maintain connectivity irrespective of their geographical positions but, such types of networks are vulnerable to various kinds of attack.

[4] The MANETs have been experiencing exponential growth in the past decade. However, their vulnerability to various attacks makes the security problem extremely prominent. The main reasons are its distributed, self-organized and infrastructure independent natures. As concerning these problems, trust management scheme is a common way to detect and isolate the compromised nodes when a cryptography mechanism shows a failure facing inner attacks. Among huge numbers of attacks, blackhole attack may collapse the network by depriving the route of the normal communication.

[5] Black hole attack is a well-known attack under which performance and efficiency of mobile ad hoc networks decreases dramatically by malicious nodes. This attack affects functionality of network by dropping data packets. Black hole attack operates based upon two different phases; first, advertising fake routes containing attacker node. Second, dropping received data packets. When it comes to route advertisement phase, operation of this attack in reactive protocols can be classified into two categories.

[6] Distributed, self-organized and infrastructure-independent nature of MANET makes it vulnerable to various kinds of attacks. Among them, a threat caused by black hole attack is more prominent. A trust management scheme is a common way to detect and isolate the compromised nodes while a cryptography mechanism shows a failure facing to inner attacks. The previous work proposed two simple models along with trust computation methods to filter out black hole nodes using the benevolent ones and achieved better performance against pure black hole attacks. In this study, a method to prevent gray-hole attack, one kind of black hole attack, which is more cunning and clandestine attack is proposed.

[7] MANETs are best suited for emergency situations as they facilitate fully distributed, self maintainable dynamic topology networks that operate without the use of external infrastructure. But the proliferation of such MANET based applications is limited as its features though impart high applicability but also manifest unreliability. Another cause of unreliability is the mutual intrinsic trust during communication.

[8] Ad hoc On-demand Distance Vector routing (AODV) is a widely adopted network routing protocol for Mobile Ad hoc Network (MANET). The design of AODV, however, paid little attention to security considerations, hence resulting in the vulnerability of such MANET to the black hole attack. On the basis of AODV, this paper proposes and implements AODV suffering black hole attack - BAODV (Bad Ad-Hoc On-demand Distance Vector Routing suffering black hole attack), which can simulate blackhole attack to MANET by one of nodes as a malicious one in network. BAODV can be regarded as AODV, which is used in MANET exited black hole attack. Based on BAODV, this paper also proposes a secure and efficient MANET routing protocol, the SAODV protocol, which aims to address the security weakness of the AODV protocol and is capable of withstanding the black hole attack. Experimental analysis shows that the SAODV routing protocol is more secure than the basic AODV.

III. PROBLEM FORMULATION

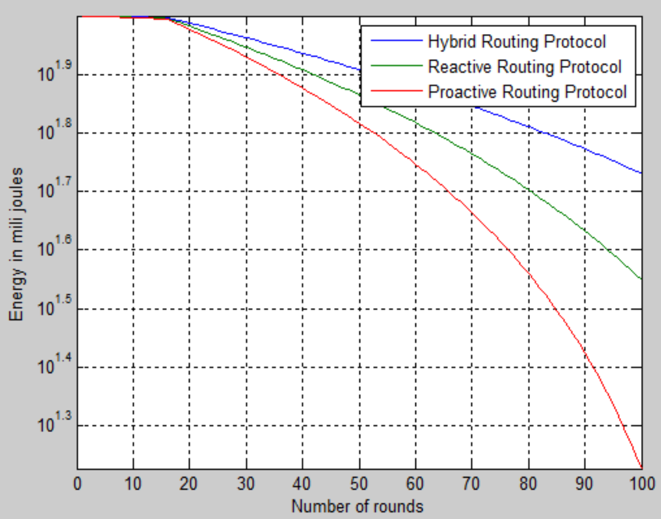
A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it.

In the Hybrid routing algorithm used by the authors in [14], they have proposed to detect the malicious nodes on the basis of the trust value. The source node will store the routes in its cache memory. The trust value of the nodes is calculated on the basis of trust factor. The trust factor of each node is calculated by taking the two parameters i.e., frequency of its usage and number of retransmissions from that node. The frequency of usage of any node is maintained in the cache memory along with the route information. The more the frequency of node in the route, the more is the trust factor. Number of retransmissions: As the number of retransmissions from any node increases, the energy required to retransmit the data also increases, thereby, resulting in less-efficient energy routing. The black hole node can occur in most of the paths available from source to destination node. Since it behaves correctly in route request phase, the number of re-transmission from this node also tends to be less. Thus the trust factor for the black hole may be high if the trust factor is calculated on the basis of above two factors. As a result, of this is chosen in the path the data packets forwarded to it will get dropped resulting in lesser packet delivery ratio and throughput of the network. Our proposed system tends to detect the black hole nodes in the network on the basis of threshold value.

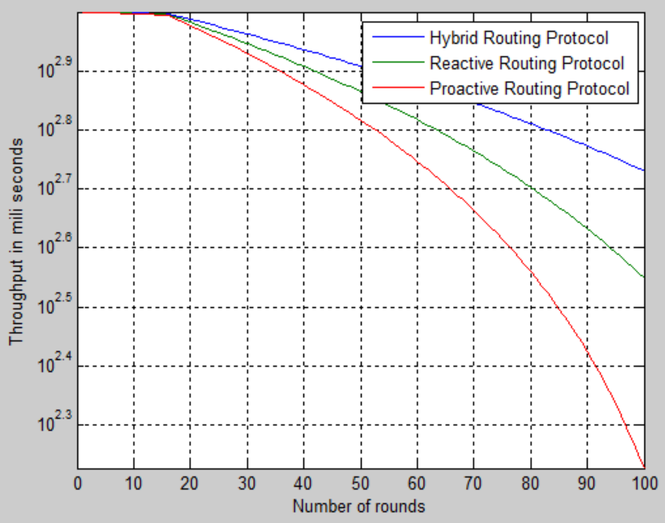
IV. METHODOLOGY

- Source node will broadcast the route request messages in the network.
- If the intermediate node have the path to destination node, then they will reply else they will re-broadcast the route request messages to the neighbours.
- When the route request reaches the destination node, it will reply to the source node via various possible paths.
- At the source node first the frequency of the node appearing in the path and number of retransmissions from it will be calculated.
- Then the trust value of the nodes will be calculated using the above two factors.
- If the trust value of a node is high but it has replied with the sequence number more than the threshold value then it will not be considered to send the data from source to destination node.
- The path will be selected whose trust value is high and the sequence number adheres to the threshold value.

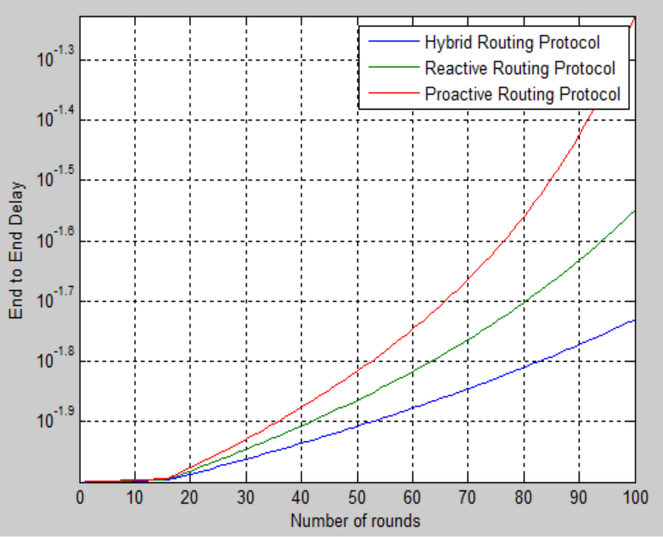
V. RESULTS



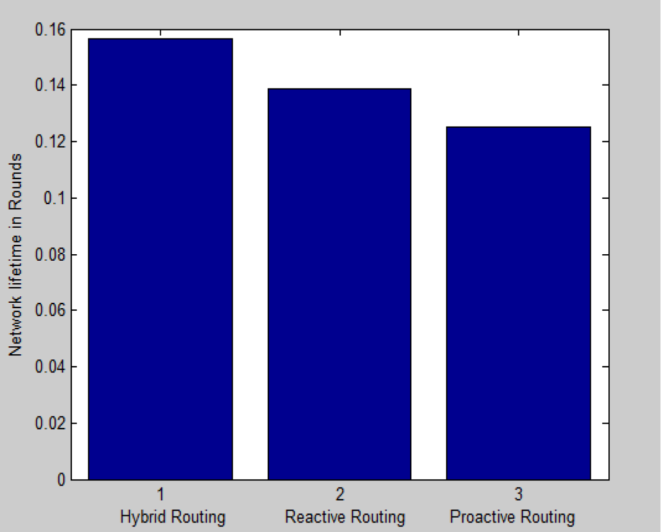
This figure shows the graph between Energy and Number of rounds.



This figure shows the graph between Throughput and Number of rounds.



This figure shows the graph between End to End Delay and Number of rounds.



This figure shows the bar graph between Reactive, Proactive and Hybrid protocol for Network lifetime.

VI. DISCUSSION AND CONCLUSION

Conclusion

This work is an enhancement of the previous work done on the bases of trust value for detection and protection of black hole attack in MANETs. In this we have simulated HYBRID protocol in MATLAB in which the Reactive and the Proactive protocols are judged. In the process we are making the main Idea of routing by firstly deploying the 500 nodes in a network and then individually making the simulation of reactive and proactive protocols for the same mechanism as we have decided for the hybrid one. The hybrid mechanism used the qualities of both reactive and proactive routing.

The route selection process starts from the source node which selects the paths by following the condition that the nodes can be used more than one time and not more than two times which enable the route selection process to be reactive and as well as proactive.

Future Scope of this work can be to test the mechanism for dynamic malicious node detection which can catch the malicious nodes during routing.

We have simulated the HYBRID and the individual protocols in MATLAB simulation. The parameters used for comparison the results are Energy consumption, Throughput, End to End Delay and Network lifetime calculated as follows.

Energy consumption

EC=EC+RE..(Eq. 1)

Throughput

TH=EI-EC/10...(Eq. 2)

Delay

DEL=Delay between packets observed......(Eq.3)

Network lifetime

NL=Rounds/ND..(Eq. 4)

Where
EC is energy consumed
RE is the routing energy
EI is the initial energy
TH is the throughput
DEL is the End to End Delay.
NL is the Network Lifetime.
ND is number of nodes deployed.

REFERENCES

[1] Raza, M. and Hyder, S.I., 2012, January. A forced routing information modification model for preventing black hole attacks in wireless Ad Hoc network. In *Proceedings of 2012 9th International Bhurban Conference on Applied Sciences & Technology (IBCAST)* (pp. 418-422). IEEE.

[2] Mishra, B.K., Nikam, M.C. and Lakkadwala, P., 2014, April. Security against Black Hole Attack in Wireless Sensor Network-A Review. In *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on* (pp. 615-620). IEEE.

[3] Aware, A.A. and Bhandari, K., 2014, October. Prevention of Black hole Attack on AODV in MANET using hash function. In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on* (pp. 1-6). IEEE.

[4] Yang, B., Yamamoto, R. and Tanaka, Y., 2014, February. Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs. In *16th International Conference on Advanced Communication Technology* (pp. 223-232).IEEE.

[5] Salehi, M., Samavati, H. and Dehghan, M., 2012, May. Evaluation of DSR protocol under a new Black hole attack. In *20th Iranian Conference on Electrical Engineering (ICEE2012)* (pp. 640-644). IEEE.

[6] Yang, B., Yamamoto, R. and Tanaka, Y., 2012, February. Historical evidence based trust management strategy against black hole attacks in MANET. In*Advanced Communication Technology (ICACT), 2012 14th International Conference on* (pp. 394-399). IEEE.

[7] Dhurandher, S.K., Woungang, I., Mathur, R. and Khurana, P., 2013, March. GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs. In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* (pp. 357-362). IEEE.

[8] Lu, S., Li, L., Lam, K.Y. and Jia, L., 2009, December. SAODV: a MANET routing protocol that can withstand black hole attack. In *Computational Intelligence and Security, 2009.CIS'09.International Conference on* (Vol. 2, pp. 421-425).IEEE.

[9] Sarma, K.J., Sharma, R. and Das, R., 2014, February. A survey of black hole attack detection in MANET. In *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on* (pp. 202-205). IEEE.

[10] Wahane, G., Kanthe, A.M. and Simunic, D., 2014, December. Detection of cooperative black hole attack using crosschecking with truelink in MANET. In *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on* (pp. 1-6). IEEE.

[11] Karuppiah, A.B., Dalfiah, J., Yuvashri, K. and Rajaram, S., 2015, February. An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks.In International Confernce on Innovation Information in Computing Technologies (pp. 1-7).IEEE.

[12] Weerasinghe, H. and Fu, H., 2007, December. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In *Future generation communication and networking (fgcn 2007)*(Vol. 2, pp. 362-367). IEEE.

[13] Ballav, B., Rana, G. and Pattanayak, B.K., 2015, December. Investigating the effect of Black Hole attack on Zone Based Energy Efficient Routing Protocol for Mobile Sensor Networks.In *2015 International Conference on Information Technology (ICIT)* (pp. 113-118).IEEE.

[14] Moudni, H., Er-rouidi, M., Mouncif, H. and El Hadadi, B., 2016, March. Modified AODV routing protocol to improve security and performance against black hole attack. In *2016 International Conference on Information Technology for Organizations Development (IT4OD)* (pp. 1-7). IEEE.

[15] Wahane, G., Kanthe, A.M. and Simunic, D., 2014, May. Technique for detection of cooperative black hole attack using true-link in Mobile Ad-hoc Networks. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on* (pp. 1428-1434). IEEE.

[16] Sardana, A., Bedwal, T., Saini, A. and Tayal, R., 2015, March. Black hole attack's effect mobile ad-hoc networks (MANET). In *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*(pp. 966-970). IEEE.

[17] Mejaele, L. and Ochola, E.O., 2015, November. Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor. In*2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)* (pp. 140-144). IEEE.

[18] Chauhan, R.K., 2015, May. An assessment based approach to detect black hole attack in MANET. In *Computing, Communication & Automation (ICCCA), 2015 International Conference on* (pp. 552-557).IEEE.

[19] Zhang, J., Liu, K., Tan, Y. and He, X., 2008, June. Random black hole particle swarm optimization and its application. In *Neural Networks and Signal Processing, 2008 International Conference on* (pp. 359-365).IEEE.

[20] Yin, J. and Madria, S.K., 2006, June. A hierarchical secure routing protocol against black hole attacks in sensor networks. In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)* (Vol. 1, pp. 8-pp).IEEE.