Azerbaijan Journal of High Performance Computing, Vol. 2, Issue 2, 2019, pp. 113-121
https://doi.org/10.32010/26166127.2019.2.2.113.121

# Comparative Study on Trust-Based Model and Black Hole Detection and Elimination in MANETs

Priya Paul[1], Satyabrata Das[1], Bata Krishna Tripathy[2], Swagat Kumar Jena[2]

[1] *Veer Surendra Sai University of Technology, Sambalpur, Burla, Odisha, India, teacher.satya@gmail.com*
[2] *Indian Institute of Technology Bhubaneswar, Odisha, India, bt10@iitbbs.ac.in, skj11@iitbbs.ac.in*

*Correspondence: Satyabrata Das, Veer Surendra Sai University of Technology, Sambalpur, Burla, Odisha, India, teacher.satya@gmail.com

## Abstract

A mobile ad hoc network (MANET) is a framework-less network consisting of several mobile nodes with wireless network interfaces. Due to node mobility in MANET, the stability of the network is affected by which the trust value of a node makes it reliable for packet transmission. The evaluation of the trust value of a node depends on three parameters, such as rank, remaining battery power, and stability factor of a node. In this paper, various trust-based models and their advantages and disadvantages have been studied. Various attacks affect the MANET from which the black hole attack is one of the security attacks. The black hole attack can be a single black hole attack or can be a cooperative black hole attack. The two properties of a black hole attack are the malicious node impersonates other nodes of having a valid route to the destination even the route is spurious and, second is the attacker consumes the packets without forwarding them. In order to combat this issue, various solutions have been studied.

**Keyword:** Trust, stability, fidelity level, Blackhole attack

### *1. Introduction*

Mobile ad hoc network (MANET) is a shared network that has no centralized infrastructure such as base stations like in wireless sensor networks (WSNs). The nodes move freely by changing the network topology dynamically, randomly, and unpredictably. Trust management is the most important issue in MANET because collecting trust information to evaluate trustworthiness is difficult due to dynamic topology changes and various attacks. The selection of the most reliable path depends upon the calculation of the trust of the nodes.

For this reason, different solutions have been proposed by different authors to provide better performance in terms of throughput, efficient resource utilization, and secure routing. As the transmission takes place in the open channel, the MANETs are susceptible to various security invasions, which reduce the performance of the network. The black hole attack is one of the most prominent attacks in MANETs in which a black hole node, i.e. a malign node, impersonates some other nodes of having

the shortest path to the nodes whose packets it wants to obstruct. There exist two types of black hole attacks i.e. single black hole attacks in which one black hole node is involved and a cooperative black hole attack in which multiple black hole nodes participate in the network. In MANETs, routing is also a challenging task, and to defeat this problem, several routing protocols have been designed, and still, the number is increasing but it is quite difficult to know which protocol is the best one to fit into the solutions of MANETs.

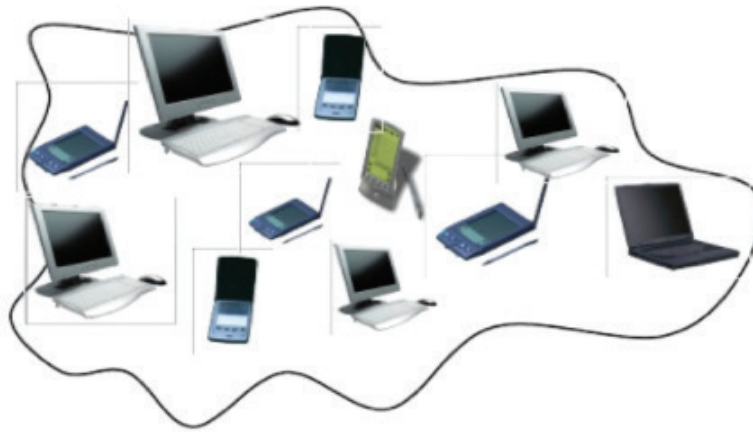


*Fig. 1: Mobile Ad hoc Network*

*Characteristics of MANETs*

*i. Dynamic network topology:* Nodes move freely, thereby, changing the network topology randomly and unpredictably.

*ii. Multi-hop routing:* When a node sends messages to another node, and it is not within the communication range, then it sends the messages via one or more intermediate nodes.

*iii. Autonomous nature:* As MANETs do not have a centralized infrastructure, so the nodes act both as host and router.

*iv. Limited battery power:* Nodes operate on small batteries having low power storage and small memory size.

*v. Relationship between nodes:* Unlike a wired network, there is no master-slave relationship.

*2. Security Attacks in MANETs*

As in MANETs, there is no centralized infrastructure so that nodes can set up the paths among themselves for packet transmission dynamically. For this, the security mechanism arises. In order to maintain a secure and reliable multi-hop environment, some security goals need to be maintained, i.e., confidentiality, availability, authentication, integrity, and non-repudiation. The security attacks in MANET are mainly divided into two categories i.e. passive and active attacks.

*Passive Attacks:*

Here the working of the network is not disturbed as the attacker only listens to the

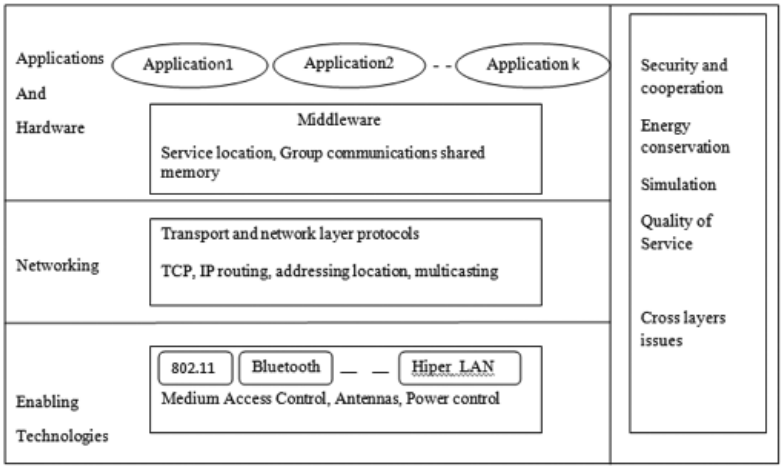



*Fig. 2: Architecture of MANET*

network without disturbing the internal environment. No data is altered or manipulated. The most suitable solution is to encrypt data being transmitted.

*Active Attacks:*

The data is altered or destroyed by the malicious node while being transmitted through the network for which the operation of the network is disrupted. According to different layers, active attacks are classified into different types. The table below shows different attacks in different layers.

*Table 1. Attacks on different layers.*

| Layers | Attacks |
|---|---|
| MAC | Jamming |
| Network | Blackhole, wormhole, IP Spoofing, Byzantine, State pollution |
| Transport | Session hijacking, SYN flooding |
| Application | Repudiation |
| Multiple layers | DoS, Link spoofing, Location disclosure, Device tampering |

*3. Related Work:*

Bo et al. (2003) proposed a neighborhood-based method. This helps to detect a black hole attack, and also a route recovery protocol was proposed to set up a path to reach a true destination. Two types of black hole attacks were focused on one is when the malign node directly attacks data traffic on the path. Another is routing control traffic in which malign node can impersonate some other nodes.

Shurman et al. (2004, April) have suggested two possible ways to combat the black hole attack. One way was to discover more than one route to the destination, and the other one was to traverse the packet sequence number included in any packet header.

Xiaoqi Li et al. (2004, March) has designed a TAODV (Trusted AODV) protocol, which is the extended version of AODV. In this, the trust among the nodes is characterized by opinion and is derived from subjective logic. TAODV gives information on trust when performs routing discovery and routing maintenance and focuses on security solutions of routing protocol in the network layer.

Elmar Gerhards-Padilla et al. (2007, October) proposed a focused approach TOGBAD (Topology Graph-Based Anomaly Detection) in tactical MANETs for detecting routing attacks using a topology graph. They triggered an alarm if the plausibility check fails.

Satoshi et al. (2007) proposed an inconsistency detection method by updating the training data at constant time intervals for analyzing a black hole attack in mobile ad hoc networks.

Tamilselvan et al. (2008) have proposed a solution to combat the black hole node by assigning a "fidelity level" to every node participating in the network, which measures the reliability of the network. In case if any node's level becomes 0, then it is considered as a black hole node and is thus discarded.

Songbai Lu et al. (2009, December) has proposed a secure and efficient MANET routing protocol, i.e., SAODV, which deals with the security problem of AODV. SAODV can efficiently combat the single black hole attack giving minimum packet loss percentage.

Zhao Min et al. (2009, May) has proposed authentication schemes which are based on two hash functions such as Message Authentication Code (MAC) and Pseudo-Random Function (PRF) to identify multiple black hole nodes and to provide safe routing by eliminating those.

Mary et al. (2010) have designed a certificate-based authentication scheme by verifying the routing messages using localized certificate chains. The proposed scheme is performed in two phases: the certification phase and the authentication phase. The designed scheme Black Hole Secure On-Demand Routing Protocol (BHS-ODMRP) has better simulation results than ODMRP.

Himral et al. (2011) have proposed an efficient solution to combat black hole attacks for AODV. The proposed solution can be used to discover secure paths and prevent black hole nodes by recognizing them with their sequence numbers.

Bindra et al. (2012, September) suggested a solution to discover multiple black hole nodes by preserving an Extended Data Routing Information (EDRI) table for each node. The table maintains the node's previous malign information to report for the gray behavior of nodes.

Mandal et al. (2013) suggested a solution based on trust and rank value of nodes. The packet is transferred through a more trusted path than the shortest path.

Siddiqua et al. (2015, January) proposed a secure knowledge algorithm that helps to detect and eliminate black hole attack by considering the packet loss. This method examines first the packet drop reason before announcing the node as a black hole node, thereby avoiding the trusted node from becoming a black hole.

Shahabi et al. (2016) designed an algorithm to discover and combat black hole attacks. An IDSAODV protocol is designed in order to overcome the problems of AODV considering throughput, packet delivery ratio, and end-to-end delay as different parameters.

*4. Trust-Based Model*

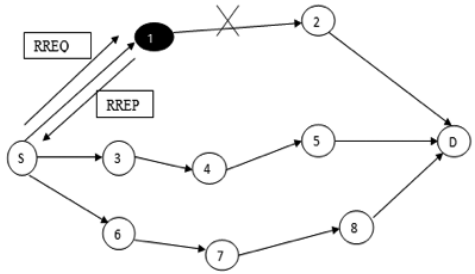
Trust is defined as the degree of belief about the behavior of various agents such as packets delivered etc. It is dynamic and decreases if agents misbehave and increase if they are doing well. Any trust management system has to be designed, keeping in mind the reliability of the system. The node having the highest trust value is considered to be more stable in the network and can be trusted for successful packet transmission.

*Table 2: Summary of advantages and disadvantages of the trust-based model*

| Authors | Advantages | Disadvantages |
|---|---|---|
| Licia Capra (2004, May) | A trust management framework is a self-adjusting infrastructure. | The issue of identification is not addressed.<br>In the future, the adaptability of the model to the user's disposition will be evaluated. |
| Xiaoqi Li (2004, March) | More flexible and less overhead routing protocol | Tolerance and overhead message schemes need to be analyzed further |
| Huaizhi Li (2007) | Ensures efficient utilization of network resources.<br>It helps in minimizing risk. | It does not consider the false recommendation.<br>Maintaining data consistency is a challenging issue. |
| Jin-Hee Cho (2010) | "Social trust" combined with "QoS trust." | Trust value is associated with a single node.<br>In the future concept of cognitive networks, the behavior will be introduced. |
| Suparna Biswas (2014, February) | High throughput and packet delivery ratio.<br>Effective black hole detection with minimum packet drop. | As the rank of a node reduces to 1 with each route discovery, sometimes a good node's rank reduces to 0; hence, it cannot take part in the transmission process henceforth. |

*5. Blackhole attack*

In this type of attack, a malign node claims to have an optimal path to the destination node. Upon receiving the request, the malign node sends a false reply with an extremely short route. Once the node can fit itself between the communicating nodes, it can do anything with the packets that are passing through it. It has two properties. First, the malicious node impersonates other nodes of having a valid path to the destination even though the route is false. Second is when the attacker engulfs the packets without forwarding. There are two types of black hole attacks single as well as cooperative, as shown in fig 3 and 4.



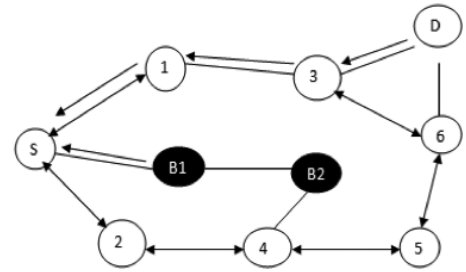




*Fig.3: Blackhole attack  Fig.4: Cooperative black hole attack*

*Table 3: Advantages and disadvantages of black hole attack solutions*

| Authors | Solutions | Advantages | Disadvantages |
|---|---|---|---|
| Bo Sun (2003) | Neighbor-hood-based method and routing recovery protocol | Detect misbehavior of black hole nodes. The number of cryp-tography operations is reduced. | Retrofitting security mechanisms are ex-pensive. Packet throughput is not improved. Routing control traffic is not effective. |
| Al-Shur-man (2004, April) | To find more than one route and to exploit the packet sequence number. | The authenticity of the node is verified by utilizing network redun-dancy. Fast and reliable in identifying the fake reply. No overhead exists. | The time delay is more as the source node has to wait for all the RREP packets. The number of select-ed routes is lower. |
| Elmar (2007, October) | TOGBAD using topology graphs. | The attack is detected immediately when the attempt is made. An alarm is triggered if the plausibility check fails. | The black hole node may influence mes-sages needed to create a graph. No concept of traffic overhead. |
| Kurosawa (2007) | Anomaly de-tection using dynamic training method. | The detection rate is in-creased using training data. An increase in the number of connections increases the packet delivery ratio. | Detection accuracy degrades when the updating time interval becomes longer. |

| | | | |
|---|---|---|---|
| Tamilselvan (2008) | Fidelity table | It provides better security and performance. | Delay in the network is more.<br>Routing overhead is more. |
| Songbai Lu (2009, December) | SAODV protocol | The exchange of random numbers verifies the destination node.<br>Security and efficiency are more than AODV. | Network overhead is more.<br>It can only withstand a single black hole node. |
| Zhao Min (2009, May) | Message Authentication Code (MAC) and Pseudo-Random Function (PRF) | Message confirmation and group recognition are fast.<br>Tackle multiple black hole nodes. | Unlimited message authentication cannot be done. |
| Mary (2010) | Certificate-based authentication | Multicast groups can withstand attacks.<br>The packet delivery ratio is more in BHS-ODMRP than in ODMRP. | End-to-end delay is more in BHS-ODMRP. |
| Himral (2011) | Sequence number concept. | The identity of the malign node is maintained as MN- Id to discard control messages coming from it. | The performance of the network is not analyzed.<br>Cannot resist multiple black hole nodes. |
| Bindra (2012, September) | Extended Data Routing Information (EDRI) table | Identify multiple black hole nodes.<br>Can know about the gray nodes also. | Malicious nodes need to be successive when in collaboration.<br>The proposed algorithm is not efficient. |
| Mandal (2013) | Trust-based routing | Nodes with high trust value have less packet loss.<br>QoS is increased. | Delay in the network increases. |
| Siddiqua (2015, January) | Secure knowledge algorithm | Prevents the trusted node from becoming a black hole node. | The re-initiating process increases the time delay. |
| Shahabi (2016) | IDSAODV protocol | Identify destructive nodes by low end-to-end delay. | Flood of information on the nodes. |

*6. Design Challenges in MANET*

i. Sensor locations: This is the challenging task because depending upon the location of sensors, the time delay is evaluated. If nodes are not within the communication range, then the messages will be transferred via one or more intermediate nodes because there is no base station concept in MANET.

ii. Energy capacity: Sensor nodes are battery-powered, so they have limited energy capacity. So energy poses a big issue for networks in an adverse environment.

iii. Node positioning: Sensor nodes can be arranged either manually or randomly that affects the performance of the routing protocols.

iv. Network characteristics and unreliable environment: The topology of the network changes dynamically because of a node failure, battery consumption making it unreliable.

v. Scalability: Communication links between sensors may not be symmetric, i.e. a pair of sensors may not be able to communicate in both directions because sensors may not have the same size, battery power etc.

*7. Conclusion*

In the above analysis, we have studied about the different trust-based models. This concept arises due to autonomous behavior in MANET. The more trusted is the node, the more suitable it is for the transmission of packets to the specified destination. The trust value is calculated by assigning a rank to each node.

Blackhole attack is a serious threat in MANETs as this attack impersonates other nodes of having a secure route to the destination. So we have done a comparative study about the black hole attack solutions, their advantages and disadvantages considering various metrics such as end-to-end delay, network overhead, throughput, etc.

*References*

Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In *Proceedings of the 42nd annual Southeast regional conference* (pp. 96-97). ACM.

Anita, E. M., & Vasudevan, V. (2010). Black hole attack prevention in multicast routing protocols for mobile ad hoc networks using certificate chaining. *International Journal of Computer Applications, 1*(12), 21-2.

Bar, R. K., Mandal, J. K., & Singh, M. M. (2013). QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack. *Procedia Technology, 10,* 530-537.

Bindra, G. S., Kapoor, A., Narang, A., & Agrawal, A. (2012, September). Detection and removal of co-operative blackhole and grayhole attacks in MANETs. In *2012 International Conference on System Engineering and Technology (ICSET)* (pp. 1-5). IEEE.

Biswas, S., Nag, T., & Neogy, S. (2014, February). Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. In *2014 Applications and Innovations in Mobile Computing (AIMoC)* (pp. 157-164). IEEE.

Capra, L. (2004, May). Towards a human trust model for mobile ad-hoc networks.

Cho, J. H., Swami, A., & Chen, R. (2010). A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials, 13*(4), 562-583.

Gerhards-Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., & Tolle, J. (2007, October). Detecting black hole attacks in tactical MANETs using topology graphs. In *32nd IEEE Conference on Local Computer Networks (LCN 2007)* (pp. 1043-1052). IEEE.

Himral, L., Vig, V., & Chand, N. (2011). Preventing aodv routing protocol from black hole attack. *International Journal of Engineering Science and Technology (IJEST), 3*(5), 3927-3932.

Jawandhiya, P. M., Ghonge, M. M., Ali, M. S., & Deshpande, J. S. (2010). A survey of mobile ad hoc network attacks. *International Journal of Engineering Science and Technology, 2*(9), 4063-4071.

Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *IJ Network Security, 5*(3), 338-346.

Li, H., & Singhal, M. (2007). Trust management in distributed systems. Computer, 40(2), 45-53.

Li, X., Lyu, M. R., & Liu, J. (2004, March). A trust model based routing protocol for secure ad hoc networks. In *2004 IEEE Aerospace Conference Proceedings (IEEE Cat. No. 04TH8720)* (Vol. 2, pp. 1286-1295). IEEE.

Lu, S., Li, L., Lam, K. Y., & Jia, L. (2009, December). SAODV: a MANET routing protocol that can withstand black hole attack. In *2009 international conference on computational intelligence and security* (Vol. 2, pp. 421-425). IEEE.

Min, Z., & Jiliu, Z. (2009, May). Cooperative black hole attack prevention for mobile ad hoc networks. In ***2009*** *International Symposium on Information Engineering and Electronic Commerce* (pp. 26-30). IEEE.

Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2016). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks, 22*(5), 1505-1511.

Siddiqua, A., Sridevi, K., & Mohammed, A. A. K. (2015, January). Preventing black hole attacks in MANETs using secure knowledge algorithm. In *2015 International Conference on Signal Processing and Communication Engineering Systems* (pp. 421-425). IEEE.

Sun, B., Guan, Y., Chen, J., & Pooch, U. W. (2003). Detecting black-hole attack in mobile ad hoc networks.

Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. *JNW, 3*(5), 13-20.

***Submitted 16.05.2019***
***Accepted 07.10.2019***