IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Survey: Detection of Blackhole Mechanism on MANET

Mr.Vishwajith M V[1], Pratik Sanjel[2], Pranish Pokharel[3], Kshetiz Pokhrel[4]

Senior Assistant Professor, Information Science & Engineering Department, NHCE, Bangalore, India[1]

Student, BTech, Information Science & Engineering Department, NHCE, Bangalore, India[2,3,4]

Abstract: A Mobile Ad hoc Network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. Protecting the network layer of a MANET from malicious attacks is an important and challenging security issue, since most of the routing protocols for MANETs are vulnerable to various types of attacks. Ad hoc On-demand Distance Vector routing (AODV) is a very popular routing algorithm. However, it is vulnerable to the well-known black hole attack, where a malicious node falsely advertises good paths to a destination node during the route discovery process but drops all packets in the data forwarding phase. This attack becomes more severe when a group of malicious nodes cooperate each other. The proposed mechanism does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to malicious activities of the nodes. Simulation results show that the scheme has a significantly high detection rate with moderate network traffic overhead and computation overhead in the nodes. Keywords-Mobile ad hoc network (MANET), blackhole, packet dropping attack, malicious node, routing misbehavior,

I. INTRODUCTION

A MANET a wireless technology growing rapidly, a network in which node sends packets from source to the destination without any infrastructure. An intermediate node is used to carry out data from sender to destination. Each node is a router and a host in MANET.

Despite the major issues in the node mobility and bandwidth constraints and error prone wireless channel, resource constrained nodes, and dynamic changing of the network topology various routing protocols have been designed to enhance the network performance i.e Proactive(table driven) and reactive(on demand) routing protocols. In tjis paper we mainly focus AODV protocol.

Due to the wireless nature of the MANET it is more vulnerable to the security attack and inherits the threats of wired as well as wireless network and the security attacks that are unique to itself.

The power capabilities make more vulnerable to the denial of service(DOS), the node mobility makes the nodes ability to distinguish the stale routes and the fake route. The malicious node either sends fake messages , not forward the packets to the destination and sending the fake routing information.

A black hole attack is a denial of service attack which occurs when a malicious node interferes in the optimal path in which the data is being transferred between the source and destination. The malicious node will consume all the packets or the data is lost. Authenticated Routing for Ad-hoc Networks (ARAN) , Secure Link State Routing Protocol (SLSP) , and Secure Ad-hoc On-demand Distance Vector routing (SAODV) ,Power and computation cost of using cryptographic techniques. Simulation studies have shown the impact of such attacks and the effectiveness of proposed defence mechanisms.

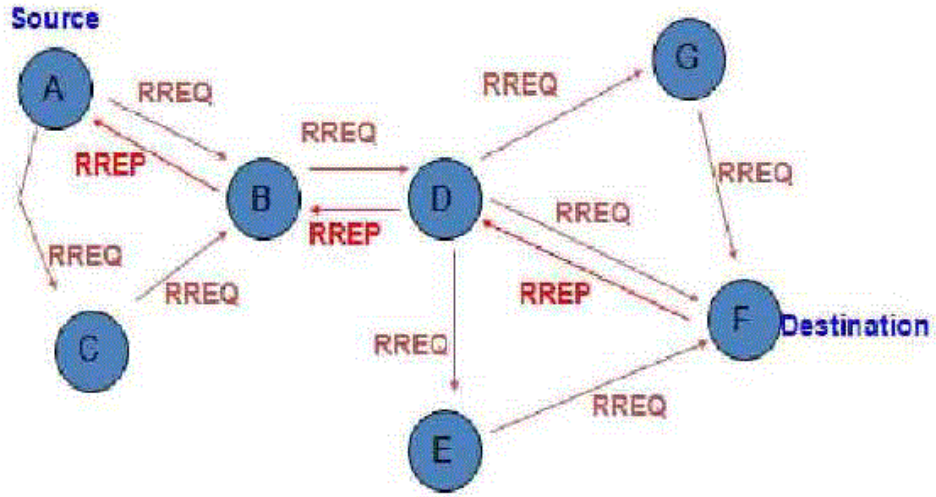
II. LITERATURE SURVEY

A. Analysis of Security Attacks on AODV Routing

All Routing protocols are vulnerable to different security attacks. Attacks can be generally divided into two categories as passive attack and active attack. Passive attack is the attacker does not affect with the normal operation of the routing protocol but only gets the information by listening to the network traffic. Active attack is the attacker modifies the exchanged data which includes removal of the information .

Black hole Attack is a type of Denial of Service Attack . Black hole Attack is a malicious node uses its routing protocol to advertise itself having the shortest path towards destination node. When route is established, then malicious node drops the packets or forwards it to the ttacker desired address

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018



The black hole attack is simulated using the NS2-2 network and also study about the effect on the performance metrics such as end-end delay, network throughput. we conclude that the black hole and flooding attacks have dramatic impact on throughput, end-delay and routing overhead. Also Gary hole attack has no affect so much on the performance and the end to end delay because both the attacks drop the data packets. But the black hole attack introduce a fake RREP which affect the network performance. . Although many researchers have worked through the security of AODV but the area of research in this is still open. Many techniques have been designed to provide security in AODV against some specific attacks. Not all the attacks can be prevented by using a single technique. So a combination of number of techniques should be used to fully secure the AODV Routing Protocol.

Advantages:

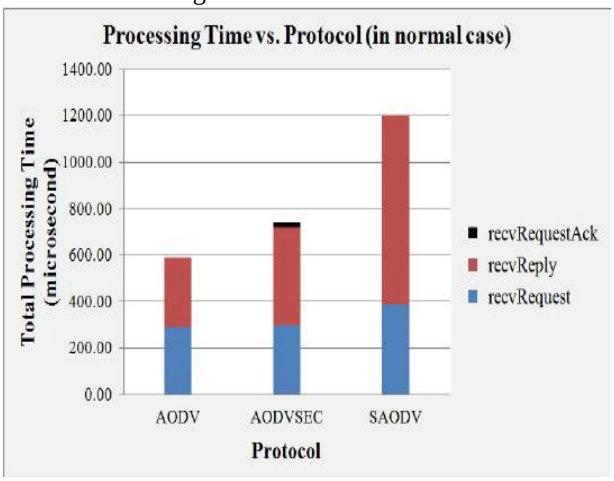
- Inherits security threats that are faced in wired as well as wireless networks.
- Flexible.

Disadvantages:

- Has a high processing demand.

B. AODV & SAODV under Attack: Performance Comparison

AODV is a reactive MANET routing protocol that does not support security of routing messages. SAODV is an extension of the AODV routing protocol that is designed to fulfil security features of the routing messages. In this paper, we study the performance of both AODV and SAODV routing protocols under the presence of blackhole, grayhole, selfish and flooding attacks. We conclude that the performance of SAODV is better than AODV in the presence of blackhole, grayhole and selfish attacks while its performance is worse than AODV in the presence of flooding attack. The blackhole and flooding attacks have a severe impact on the AODV and SAODV performance while the grayhole and selfish attacks have less significant effect on it.



IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

The performance comparing to both SAODV AND AODV ,SAODV has the better performance than AODV in the black hole. Since SAODV does not forward the packets without ensuring the intergrity that reduce the routing packet which may cause congestion .SAODV is not better than AODV in presence of flooding attack and also cannot better in finding the malicious node

Advantages:

- Reduces the routing packets that may cause congestion.
- Performance of SAODV is better than AODV in the presence of blackhole, grayhole and selfish attacks.
- Provides an end to end authentication of the route and node by node verification of routing messages, using asymmetric cryptography and has chaining.

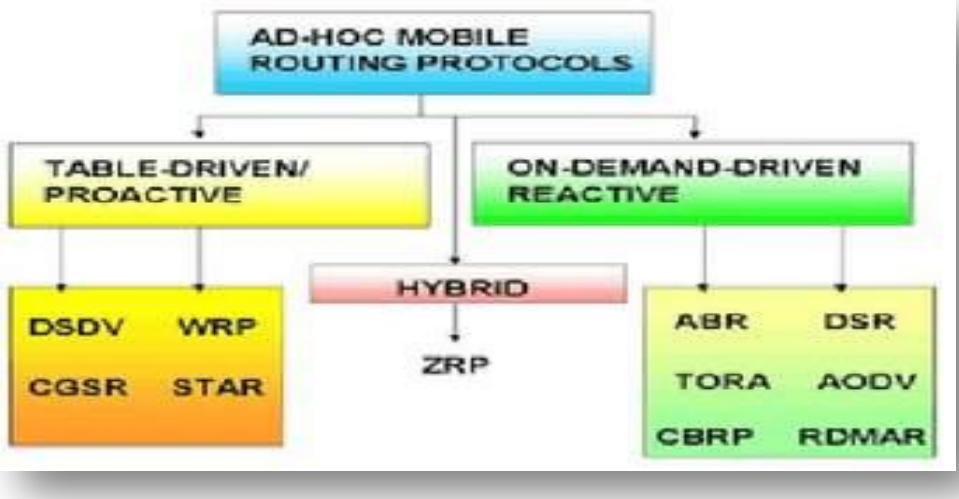
Disadvantages:

- Performance of SAODV is worse than AODV in the presence of flooding attack.
- Malicious nodes impersonating non-existent nodes which cannot be discovered by other non-malicious nodes.
- Affects the network performance.

C.Routing protocols in ad hoc networks: A survey

As we know ad hoc is a Network which has a dynamically changing topology which has no fixed infrastructure. In the ad hoc network there is no fixed infrastructure and has no centralized administration. In the ad hoc environment the bandwidth is constrained in wireless links. The ad hoc environment contains energy constrained nodes.

We had introduced a taxonomy of ad hoc routing protocols in this paper.Ad hoc routing are divided in nine categories: (i) source-initiated (reactive oron-demand), (ii) table-driven (pro-active), (iii) multipath, (iv)location-aware (geographical), (v) hybrid, (vi) multicast,(vii) geographical multicast, (viii) hierarchical, and(ix) power-aware.Compared several representative protocols had been reviewedand for each of these classes.Under different scenarios we can operate several classes of protocol,Common goal are shared between them to reduce controlpacket overhead, maximize throughput, and minimizethe end-to-end delay. The ways of finding and/or maintainingthe routes between source–destination pairs is the main factor between the protocols.As well as this can create a serious problem. We can requires a very careful analysis of the Scenario and its requirements for deploying of ad hoc network with an optimal performance, and from dozen of applicable in the context the appropriate choice of the routing protocol. This paper taxonomy presented will be a helpful instrument for making this decision.



Advantages:

- Reduce controlpacket overhead, maximize throughput, and minimizethe end-to-end delay.
- Escape as quickly as possible from the challenges of wireless domain and enter the reliability of fiber optic networks and time-tested networking protocols.
- Connect to an access point which usually has a wired connection to the Internet.

Disadvantages:

- Cannot identify a single‘‘best’’ protocol.
- Limitations in transmission range, cost or access rights considerations.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

D. Robust Routing in Wireless Ad Hoc Networks

Wireless network is used wide due to advance of mobile device technology. Mobile devices improved and there still have some restrictions. i.e.small memory, limited CPU, and exhaustible battery. For resource-demanding operations, they are inadequate. Mobile nodes collection which do not rely on the predefined infrastructure is a wireless ad hoc network. No administrative nodes Are there to control the network, and every node participating in the network should be responsible for the reliable operation of overall network. Since each node node within the range can access it. In this infrastructure less environment, each node in ad hoc networks shows behaviors as a router to establish end-to-end connections. Also, since bandwidth is a scarce resource in wireless environment, routing efficiency shows more critical character in ad hoc networks.

No administrative node is in wireless ad hoc networks, most network algorithms are based on the collaboration between nodes. In order to cooperate with each other, trust between nodes is essential though it is hard to achieve in practice. Wireless ad hoc network is inherently vulnerable. On the other hand, the transmission medium itself necessitates security in wireless ad hoc networks. Therefore, we need the security consideration in wireless ad hoc Network.
A new scheme was introduced to add the route confirmation request and reply response paths and that strengthens the robustness of routing information .Simulation results validate the effectiveness of our protocol against blackhole attack. With malicious nodes, delivery ratio of our protocol stays as high as 80% while Dynamic Source Routing(DSR) protocol delivers less than 50% of data packets sent. Data transmission overhead is also reduced by 10% compared to DSR, and in case of no malicious attempt, our protocol incurs only 5% additional control overhead. We note that there is only small difference between EXACT and DIFF_ONE. We will examine the behaviour of our protocol with other on-demand routing protocols such as AODV.

Advantages:

- Strengthens robustness of routing information in ad hoc networks.
- Effectiveness of protocol against the blackhole attack.
- Delivery ratio of our protocol stays as high as 80%.
- Data transmission overhead is also reduced by 10% compared to DSR

Disadvantages:

- DSR delivers less than 50% of data packets sent.
- Leads to considerable difference in overall performance in more volatile and dynamic environment.

E. Secure Link State Routing for Mobile Ad Hoc Networks

Mobile Ad-hoc Networking(MANET) is a self-organizing technology which is vulnerable to security attacks which disrupts routing protocol and disables the communication. Many protocols have been proposed to secure the MANET topologies. when a source node needs to route packets to a destination these protocols are designed to perform route discovery they are reactive routing protocols. In some cases where low to medium mobility and high connection rate proactive discovery is efficient. hybrid routing protocols which are the middle ground, have been shown to be capable of adapting their operation to achieve the best performance under differing operational conditions through locally proactive and globally reactive operation. In this paper, we study a proactive MANET protocol that secures the discovery and how to provide secure proactive routing and we propose the distribution of link state information across mobile ad hoc nodes and provide informations to link state and failures of individual nodes. The distance vector protocols are affected by a single malicious node where as the link state protocol provides robustness. Link state has the ability to determine route simultaneously across multiple routes, the utilization of the local topology for transfer of data, efficient propagation of control traffic.

Secure Link State Protocol (SLSP) for mobile ad hoc networks, is presented which is robust against individual attackers. SLSP shares security goals and bears some resemblance to secure link state routing protocols. In MANET, all nodes are expected to equally assist the network operation and the node does not stem out of the connection. A secure link state protocol (SLSP) for mobile ad hoc networks is presented. the use of Neighbor lookup protocol(NLP)and the secure neighbour discovery secures the SSLP from the intruder and can operate with minimal or no interactions with a key management entity, where the network nodes are necessary to validate the peers information of connectivity. For any reason the securing of the locally proactive topology discovery process by SLSP can be beneficial for MANET. The security mechanisms of SLSP can adapt to a wide range of network conditions, and thus retain robustness along with efficiency.

Advantages:

- Secure link state protocol (SLSP) for mobile ad hoc networks.
- Use of NLP strengthen SLSP against attacks.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

- Operate with minimal or no interactions with a key management entity.
- Adapt to a wide range of network conditions, and thus retain robustness along with efficiency.

Disadvantages:

- Attempt to exhaust network and node resources.
- Opens the network to numerous security attacks that can actively disrupt the routing protocol and disable communication.

F. Detection of Malicious Attack in MANET A Behavioral Approach

A wireless ad-hoc network is a network which does not depend on an infrastructure, such as routers in wired networks as well as a decentralized network where a set of mobie devices communicate with each other. Wireless ad-hoc network topology is unreliable and dynamic. MANET uses multi hop peer to peer routing to give network connection as an alternative for fixed network infrastructure. Each node acts as a router in MANET and frontward traffic from other nodes. A the nature of MANET topology is dynamic the routing mechanism is more convuated and anxious and are more predominant to compromise and suspect of DOS denial of service attack. launched by malicious nodes or factious node. Multiple layer security is used in sodern security ans is based on the idea of defense in depth to thwart network from malicious nodes and requires a secure comunication. Proposed method presents a behavior based method to detect malicious node attack, which is based on AODV. It is a well recognized and popular reactive protocol used in MANET. Some of the attacks proposed in this paper are:

A. Service of Denial Attack (DoS) The denial of service (DoS) attack launched by the hacker inserting packets into the networks to mislead network resources. A node generates route request packets and floods them in the MANET, the bandwidth is effortlessly seized by the malicious node.

B. Black Hole A selfish node that drops the packets and and transmits further .A malicious node diverts the destination by sending wrong RREP (route reply) that it has a latest route with the less hop count to destination and then it drops the receiving packets.

C. Gray Hole A malicious node drops the packet and keeps it with them Gray Hole attack is slow poison in the network side that is the probability of packet loss is undetermined. As soon as the packets start to arrive In this attack a malicious node behave as truthful node during route discovery process and starts dropping the packets silently.

We have found many threats and countermeasures for ad-hoc wireless network. The review shows the attacks and the countermeasures to avoid and protect the network resources. A solution scheme to detect malicious node is proposed using the concept of SVM The behavior metrics are used to develop the security system those are easily computed and classify implemented using NS-3 Simulator, which is easy to understand and fast. In future this algorithm can be implemented to other reactive protocol.

Advantages:

- Knowledge of various wireless adhoc network attacks and its countermeasures.

Disadvantages:

- Loss of packets to know the countermeasures.

G. Security issues in routing protocols in MANETs at network layer.

Mobile Ad-hoc Network (MANET) is the network which was emerged for wireless communications in new way. One fixed access point is not required for MANET as like in wired network. Nodes which are kept alternative will form a network which is an active individual setup network. The communicating can host himself in this for working actively and discovering other hosts to communicate in MANET. Here one node can appoints another nodes for advancing packets within area. Wireless mobile can host the functions like a node. Router advancing packets in the network that may not be within the direct communication ambit of each other for another wireless mobile hosts. All the instrument of MANET enjoys part in an ad-hoc routing protocol. As well as it acknowledge to find out differing multi-hop ways by the help of network to any other aiding host. MANET's plays a greater role for military operations and at the time of natural collapse. MANET too have allots of security threats like other networks. For both wired and wireless networks it have common security challenges. Due to wireless network it is tough to locate which node playing malicious role, wilfully drop of valuable packets and junk packets at the time of attack.

MANET characteristics which distinguish it from other networks are like; Fluctuating Link Bandwidth, Autonomous Behaviour, Dynamic Network Topology, Multi-hop Radio Relaying, Limited Energy Resources, Distributed

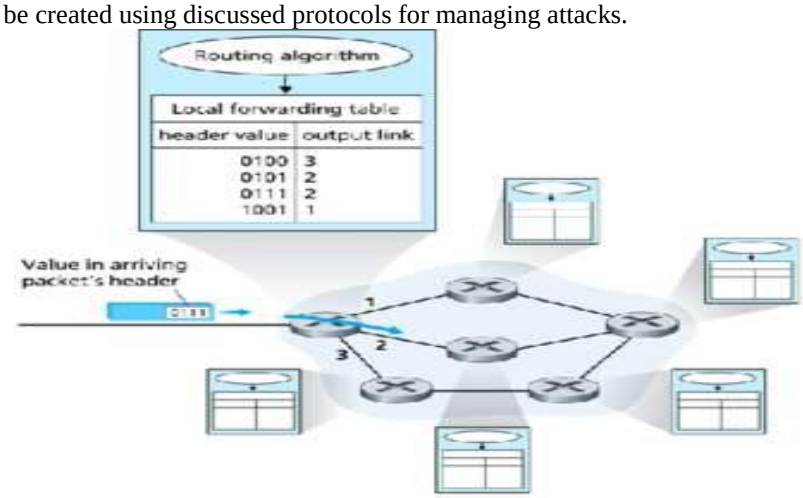
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Operations. Within accessible wireless instrument ambit via wireless links, while those are not in direct ambit necessarily rely on in between nodes to act as routers to send information and this entire working is backed by its multi-hop traits, nodes can transmit straight forwadly. It is must necessary for MANET's to be aimed at secure routing, transfer protocols, easy discovery of node when any instrument needs to pair, Bi-directional transmission between hosts and in last should be focused towards Quality of services. MANET gives access to data and services maintaining their position in network. It is not a centralized network, more flexible and also less expensive like others.

In This paper we concludes there are rely attacks against MANET's upon which transmission layer is targeted, environment in which attacks is started and the level of Ad-hoc network tool aimed. There are more features of attacks that should be reviewed before crafting any security plan for an Ad-hoc network. Because of open nature of mobility and media, MANET is extra vulnerable to security threats as described. Therefore, MANET requires greater security compared to traditional wired networks. Subsequently few secure protocols were covered for resolving security issues. A new framework can be created using discussed protocols for managing attacks.



Advantages:

- In This,due to presense of security routing protocols it makes them more secure and error free.
- Security threats in mobile ad hoc networks challanges and solutions have been overviewed.
- Network layer is most vulnarable than all others layer in MANET.
- Security are ensured for entire system.

Disadvantages:

- In this Ad hoc routing protocols,nodes are also routers because of it compromised node can give bad information for ridirecting traffic or simply stop them.
- Infrastructure of ad hoc networks are not pre determined the nodes organization start changing.
- They Will Directly Allows malicious nodes to operates which implicit trust relationship between neighbours.

H. Preventing black hole Attack in Aodv using timer-based detection mechanism

Mobile ad hoc network is one of the wireless network structures in which all nodes are movable and have topology which changes dynamically. It represents complex distributed system that consists of collection of wireless mobile nodes, which are connected through wireless links. MANET is group of decentralized mobile nodes which does not rely on any fixed infrastructure, so MANET is an infrastructure less ad hoc networks. In MANET nodes itself works as router for communication within the network. Due to mobility and low cost, a MANET is suitable for applications such as campus networks, military service, vehicle networks, casual meetings, disaster relief robot networks, emergency operations, maritime communications, and so on. Routing in MANETs is error prone due to mobile nodes and dynamic topology as compared to conventional routing protocols. In addition to this battery power and limited bandwidth is also a challenge. Earlier researchers on route establishment in MANET have their main focus on the efficiency and assume that no node is malicious, so all nodes are trustworthy. But in present scenario more,The goal of the proposed solution is the avoidance of black hole attack by detection of the malicious attacker using timer based detection approach. In this approach each node defines a trust value for its neighbor and inserts a timer with each data packet, if the trust value decreases below a threshold value for any node then all other nodes put that node in their blacklist table.

In this paper ,some how the time have been reduce for finding the malicious node but it doesn't guarantee in reventing the black hole attack. We have modified the existing code of AODV protocol according the black hole attack procedure and to the proposed Timer-based Detection method to remove a black hole node from network. Based on the simulation

results obtained, we can conclude that the proposed attack causes great damage to the network performance by ropping a large percentage of data packets that are destined to a specific destination node. The network performance degrades further with the increase in the number of attackers in the network because it increases the chances that the attacker will become part of the discovered routes. Once this is the case the attack is done on the active flows by the attackers which results in packet drops, thus decreases the network performance.

Advantage :

- The time is reduce for sending the packet to its neighbor nodes

Disadvantage:

- We can conclude that the proposed attack causes great damage to the network performance by dropping a large percentage of data packets that are destined to a specific destination node.

CONCLUSION

In this survey paper we found that ,the reactive detection method eliminates the routing overhead problem from the event-driven way, but suffered from some packet loss in the beginning of routing procedure. Therefore, we recommend that a hybrid detection method which combined the advantages of proactive routing with reactive routing is the tendency to future research direction. However, we also discover that the attacker's misbehavior action is the key factor. The attackers are able to avoid the detection mechanism, no matter what kinds of routing detection used. Accordingly, some key encryption methods or hash-based methods are exploited to solve this problem. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

REFERENCES

[1] M. A. Abdelshafy and P. J. King. Analysis of security attacks on AODV routing. In 8th International Conference for Internet Technology and Secured Transactions (ICITST), pages 290–295, London, UK, Dec 2013.
[2] M. A. Abdelshafy and P. J. King. AODV & SAODV under attack: performance comparison. In ADHOC-NOW 2014, LNCS 8487, pages 318–331, Benidorm, Spain, Jun 2014.
[3] N. Choudhary and L. Tharani. Preventing black hole attack in AODV using timer-based detection mechanism. In International Conference on Signal Processing And Communication Engineering Systems (SPACES), pages 1–4, Jan 2015.
[4] P. Joshi. Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 3:954–960, 2011.
[5] S. Lee, B. Han, and M. Shin. Robust routing in wireless ad hoc networks. In International Conference on Parallel Processing Workshops, pages 73–78, 2002.
[6] P. Papadimitratos and Z. J. Haas. Secure link state routing for mobile ad hoc networks. In Symposium on Applications and the Internet Workshops, pages 379–383. IEEE Computer Society, 2003.
[7] M. Patel and S. Sharma. Detection of malicious attack in MANET a behavioral approach. In IEEE 3rd International on Advance Computing Conference (IACC), pages 388–393, 2013.