Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

SS-AODV: Sink Secure Ad-hoc on-demand Distance Vector Routing for Wireless Mesh Networks

Er.Pushpender*
CSE, Shri Venkateshwara University, Gajraula(UP),India

Dr. Sohan Garg
CSE, C.C.S. University, Meerut, India

Abstract— Wireless Mesh Network is a collection of wireless nodes communicating among themselves over multi-hop paths. WMNs are self-configuring, self-organizing confederation of wireless systems. The Wireless Mesh Networks security is a big challenge for us. Sinkhole attack is one of the most severe security threats in WMNs that can disrupt majority of routing communications. In this paper, we have proposed SS-AODV, a sink secure routing algorithm that detects the presence of sinkhole during route discovery process and quarantines it. SS-AODV identifies route requests traversing a sinkhole and prevents such route from being established. SS-AODV uses a trust model to determine the necessary and sufficient condition for identifying a sinkhole free path. The trust model is integrated into the Ad-hoc On-demand distance vector routing protocol. At last of this paper, the performance of the proposed algorithm is analyzed by comparing the simulation results of SS-AODV with AODV in presence of

Keywords— WMNs, SS-AODV, Malicious Nodes, Sink hole, RREQ, RREP, Classifier

I. INTRODUCTION

Wireless Mesh Network is a popular technology as compared to other existing technologies. A mesh topology is used in the structure of Wireless Mesh Networks in which wireless nodes are connected to each other. Several routing protocols are used in WMNs for communication purposes. Regarding performance of WMNs, security is an important factor. Security in WMNs is a challenging issue due to open nature of the wireless medium and multi-hop cooperative communication environment. Several factors are responsible for making the network services more vulnerable, specifically due to chances of attacks from within the network. The security factor within routing protocols is a most important part in WMNs. A several number of attacks such as wormhole attack, Sybil attack, black hole attack, sinkhole attack may take place in WMNs. These attacks in the network degrade the performance and make the communication more complicated. Sinkhole attack is one of the attacks which also affect the performance of routing protocols such as AODV, DSR etc. Sinkhole attack is a attack in which an attacker tends to attract all the data which is sent by its neighbours. In this attack, a malicious node advertises wrong information to produce itself as a specific node and receives whole network traffic. Such malicious node can modify the necessary information such as changes made to data packet or drops them to make the network complicated. Such node can attract all the data from all neighbouring nodes. Sinkhole attack affects the protocols such as AODV by using flows as maximizing the sequence number or minimizing the hop count. In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate. In DSR protocol, sinkhole attack modifies sequence number in RREQ. A sinkhole attack degrades the overall performance of the routing protocols such as AODV and DSR. Hence a sinkhole secure mechanism has to be needed to prevent the network. For this, we propose a new routing algorithm SS-AODV (Sink Secure AODV) which is integrated in a trust model.

This paper addresses a particularly devastating form of attack called sinkhole attack. Present paper also addresses the trust-based routing in WMNs. The routing algorithm must react according to topological changes as per the degree of trust of a node. Trust may be referred as belief or reputation of one node or entity to perform an action. In the present paper, a trust model is integrated into the AODV routing protocol to address the sinkhole in WMNs. We present a novel routing protocol SS-AODV that addresses sinkhole attack in WMNs.

II. WIRELESS MESH NETWORK ROUTING PROTOCOLS

Several numbers of routing protocols are used in WMNs for communication purposes. WMN routing protocols are classified as: (i) Reactive routing protocols (ii) Proactive routing protocols (iii) Hybrid routing protocols. In proactive routing protocols, routing tables are updated by refreshing the continuous information. The main goal is to maintain up-to-date information in routing table. DSDV (Destination Sequenced distance vector), CGSR (Cluster head Gateway Switched Routing), OLSR (Optimized Link Static Routing) etc are the examples of proactive routing protocols. Reactive routing protocols are the on-demand based protocols in which when a route is calculated, it is stored and used until the destination is available or the path's time is out. Some examples of reactive routing protocols are: DSR (Dynamic Source Routing), AODV (Ad-hoc On-demand Distance Vector), LQSR (Link Quality Source Routing), and TORA (Temporally-Ordered Routing Algorithm). Hybrid routing protocol combines the best features of both proactive and reactive routing protocols. The routing is initially established with some proactively routes and then serves the demand

from additionally activated nodes through reactive flooding. The examples of hybrid routing protocols are: ZRP (Zone Routing Protocol), HSLS (Hazy-Sighted Link State) Routing algorithm etc.

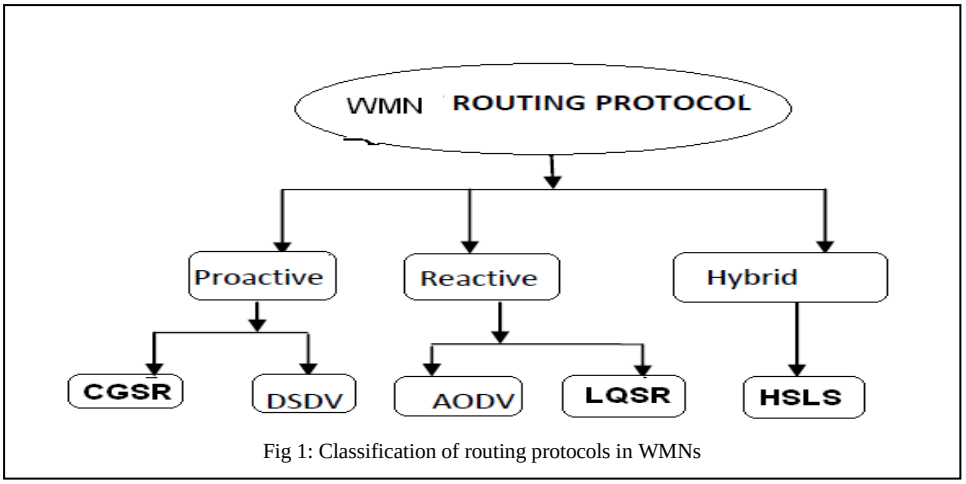

Fig 1: Classification of routing protocols in WMNs

III. REACTIVE ROUTING PROTOCOL

A. AODV Routing Protocol

A node that has a route to the destination with a higher sequence number than the one specified in the RREQ unicasts a route reply (RREP) packet back to the source.

Upon receiving the RREP packet, each intermediate node along the RREP routes updates its next-hop table entries with respect to the destination node, dropping the redundant RREP packets and those RREP packets with a lower destination sequence number than one previously seen.

When an intermediate node discovers a broken link in an active route, it broadcasts a route error (RERR) packet to its neighbours, which in turn propagate the RERR packet up-stream towards all nodes that have an active route using the broken link. The affected source can then re-initiate route discovery if the route is still needed.

AODV Properties:

- AODV does not attempt to maintain routes from every node to every other node in the network; Routes are discovered on an as-needed basis and maintained only as long as necessary.
- AODV is loop free at all times, even while repairing broken link.
- AODV is able to provide unicast, multicast and broadcast communication ability.
- AODV currently utilizes only symmetric links between neighboring nodes. AODV is capable of operating on both wired and wireless media.
- Route tables are used by AODV to store pertinent routing information.
- AODV is able to maintain both unicast and multicast routes even for nodes in constant movement.

AODV Unicast Route:

The basic outline of the route discovery process is as follows:

- When a node needed a route, it broadcast a RREQ (Route Request).
- Any node with a current route to that destination cans unicast a RREP (Route Reply) back to the source node.
- Route information is maintained by each node in its route table.
- Information obtained through RREQ and RREP messages is kept with other routing information in the route table.
- Sequence numbers are used to eliminate stale route.
- Route with old sequence numbers are aged out of the system.

AODV Unicast Route Discovery

To begin a route discovery, when a node wishes to send a packet to some destination without a route, the source node create a RREQ packet, which contains the source node's IP and current sequence number as well as the destination's IP address and last known sequence number. The RREQ also contains a broadcast ID, which incremented each time the source node initiates a RREQ. After broadcasting the RREQ packet, the node sets a timer to wait for a reply. When a node receives a RREQ, it first checks whether it has seen it before (for a specified length of time) by noting the source IP address and broadcast ID pair. If so, discards the packet.

To process the RREQ, the node sets up a reverse route entry for the source node in its route table. This reverse route entry contains the source node's IP address and sequence number as well as the number of hops to the source node and the IP address of the neighbour from which the RREQ was received. In this way, the node knows how to forward a RREP to the source if one is received.

AODV Multicast Forward Path Setup

If a node receives a join RREQ for a multicast group, it may reply if it is a router for the multicast group's tree and if its recorded sequence number for the multicast group is at least as great as that contained in the RREQ. Naturally, the group leader can always reply to a join RREQ for its multicast group. The responding node updates its multicast route table by placing the requesting node's next-hop information in the table and then generates a RREP. The node unicasts the RREP back to the node indicated in the RREQ. As nodes along the path to the source node receive the RREP, they set up a forward path entry for the multicast group in their multicast route table by adding the node from which they received the RREP as a next hop. Then they increment the Hop Count Field and forward the RREP to the next node.

AODV Multicast Route Activation/Deactivation

The source node must wait the length of the route discovery interval before using the route. If the request is to join the tree, the RREPs set up potential branches. The selected path to the tree must be explicitly activated at the end of the discovery interval so that one of these paths may be grafted onto tree. Similarly, RREPs for a non-join request set up paths to the multicast tree. During the discovery interval, the source node keeps track of the route with the greatest multicast group sequence number and the smallest hop count to the multicast tree. At the end of the discovery interval, it activates that route by unicasting a multicast activation (MACT) message to its selected next hop and by setting the Activated flag for that entry in its multicast route table. Once the next hop receives this message, it activates the route and, if it was not the originator of the RREP, then sends its own MACT message to its next hop. This continues until the originator of the RREP is reached. At that point, the new path to multicast tree has been determined.

AODV Multicast Tree Maintenance

Unlike in the unicast scenario, however, a link break necessarily triggers route reconstruction because the multi cast members must remain connected during the group's lifetime. Multicast tree maintenance takes two forms: repairing a broken tree branch following a link break, and reconnecting the tree after a network partition. Link Breaks Node may notice a link break on the multicast tree in one of two ways. If no data packets have been sent recently, a node must receive a broadcast from each of its next hops at every hello_interval. Failure to receive any broadcasts from a next hop on the multicast tree for

hello_life= (1+ allowed_hello_loss) * (hello_interval)

indicates that the next hop is out of transmission range and so the link must be repaired.

When a link break occurs, the (member) node downstream of the break (i.e., the node that is father from the multicast group leader) is responsible for repairing it (to avoid the loop). The downstream node initiates the repair by broadcasting a join RREQ (expanding ring search may be used here) for the multicast group which includes an Extension field indicating the sending node's distance from the group leader. Only nodes on the multicast tree that are at least this close to the multicast group leader may reply to the RREQ. This prevents nodes on the same side of the break as the initiating node from responding, thereby ensuring that a new route to the group leader is found.

A multicast tree member from one partition will know that it has new connectivity to another partition if it receives a Group Hello (GRPH) for the multicast group that contains group leader information difference from its own records.

For this purpose, the GRPH message is periodically broadcast by the multicast group leader across the network. It contains the IP address of the group leader and the IP address and current sequence number of the multicast group for which it is the group leader.

A repair of the multicast tree is initiated by the group leader with the lower IP address (to avoid the loop).

B. Routing Attacks in Wireless Mesh Networks

Routing attacks are grouped into two types: Passive attacks and Active attacks.

Passive attacks are those, wherein the attacker indulges in eavesdropping or monitoring of data transmission. Passive attacks don't involve any modifications to the contents of an original message. Unlike passive attacks, the active attacks are based on modification of the original message in some manner or the creation of a false message. These attacks can't be prevented easily. However, they can be detected with some effort and attempts can be made to recover from them [1]. There are several types of routing attacks in wireless mesh networks such as DOS (Denial of Services) and flooding, wormhole attack, message suppression attacks, fabrication attacks, alteration attacks, impersonation or spoofing, Sybil attacks, sinkhole attacks, black hole attacks.

Here, we will explain sinkhole attack in detail.

In this type of routing attack, a sinkhole node or a malicious node tries to attract the data from all its nearby nodes in the network. It creates wrong information and transfers this information to all its neighboring nodes. A sinkhole node receives whole network traffic and modifies the information. Due to sinkhole attack, several problems may be generated such as increasing the network overhead, decreasing life time network, and finally destroy the network. By maximizing the sequence number or minimizing the hop count, a sinkhole attack can degrades the performance/efficiency of routing protocols such as AODV (Ad-hoc On-demand Distance Vector) routing protocol. By applying such types of activities, the sinkhole node seems to be the best available route for the nodes to communicate in the network. In DSR routing protocol, a sequence number of RREQ message is modified by the sinkhole node. A sinkhole node analyze the source node's sequence number, and creates bogus RREQ message by selecting source, destination and a large sequence number than analyzed source sequence number. In AODV routing protocol, a sinkhole node may send Route Reply (RREP) messages for every Route Request (RREQ) messages and make the other nodes forward their packets towards it. It may then sink the receiving packets. After receiving the packets, it forwards them to some different route or obtains

unauthorized access to the contents of the received packets. No proper security mechanism is available by the basic AODV routing protocol.

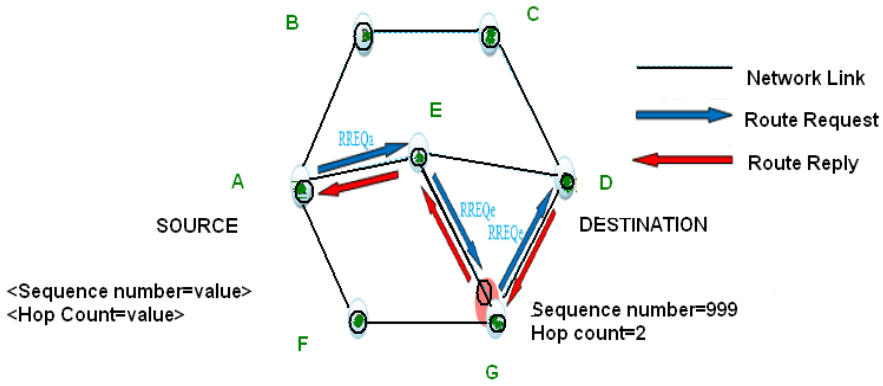

Fig. 2 Sinkhole attack in AODV

In the diagram, a sinkhole node G is shown which seems like other node in the network. This sinkhole node G advertises itself to neighboring nodes. A greater sequence number is sent to neighboring node E to create confusion that it fresh route for number of hop count value is sent by G, to tell this is shortest path. Node E supposed that the path through G is the best shortest path and initiates data packets to the destination through it. Here, two types of messages RREQ and RREP takes place for communication purposes.

C. Trust Model

The model considers the recommendation of trustworthy neighbors and the experience of the node itself. In this model, our goal is to provide the nodes with a trust level for each node that is within the radio range. The aim is to provide the features to each node capable of collecting information to reason, learn, and make their own decisions. The present model builds a trust relationship among the nodes of a Wireless Mesh Networks. This model provides a mechanism to analyze the trust level of its direct neighbors. Our trust model is made on the basis of Learning layer (Learning plan) and Trust layer (Trust plan). Trust layer and Learning layer can communicate with application layer, transport layer, network layer, link layer, physical layer of OSI model. Trust plan having several components such as Trust Table, Trust Calculator, Recommendation Calculator, and Recommendation Manager. The main functionality of the Trust plan is to define how to assess the trust level of each nearby node on the network using the information provided by the Learning plan and the information exchanged with the nodes within the radio range (i.e. direct neighbors).

A trust Table is maintained by each node. On the Trust Table, a node stores the opinion of its neighbors about their common neighbors. A timeout is integrated within each Trust Table. The variance of each Trust Table is maintained in the ATT (Auxiliary Trust Table). The addition information is supplied by the ATT. The main functionality of recommendation Manager is to receive, send, store recommendations. The recommendation process is completed into two actions. First, it is stored in ATT and after this forwarded to the Recommendation Calculator. All the recommendations are computed by the Recommendation Calculator for a particular neighbor. The Trust Calculator analyzes the trust level. The Learning plan consists of several components such as Classifier, Behavior Monitor, and Experience Calculator. It is the responsibility of the Learning layer to gather and convert information into knowledge, also to monitor and judging other's neighbors actions. The quality of an action is decided by the Classifier. When a new neighbor arrives, it is not necessary to identify it by a node. But nodes must be able for identification of neighbors that they already know. In our model, a certification authority needs not to be required. The neighbor's actions are monitored by the Learning plan.

In this model, there is no requirement to distribute the trust information over the whole wireless network, but needs only to keep and exchange trust information about nodes within the radio range.

D. Trust based mechanism concepts

- Trust is a mechanism for reducing the level of risk in a situation.
- Trust is a charge or duty imposed in a faith or as a condition of a relationship.
- Trust is a belief that is evaluated by the individuals.
- Nature of trust is subjective.
- The relationships in trust are not absolute.
- Relationship of trust is not symmetric i.e. X's trust in Y may not the same as Y's trust in X.
- In normal condition, trust is a non-transitive property, but it may be transitive when one assumes the use of recommendations and delegation. The following statement explains this concept: If A trust B and B trust C, then A trusts C. This conditional statement is in normal form is not true, but may be assumed true if the some conditions are true as given below:
    - B explicitly tells A that he trusts (recommendation).
    - A trusts B as a recommender. A doesn't trust B as a recommender then he should ignore information B supplies him with.

- A must be allowed to make a judgement on the quality of B's recommendation.

- Every node in a network assigns a level of trust for each nearby node i.e. neighbour.
- There is a level of trust associated with a relationship.
- In our proposed approach, nodes interact only with its nearby nodes. Hence, it is need not require keeping trust information about every node in the network. As a result, lower energy consumption, less processing for trust level calculation and less memory space is required.
- Trust value is evaluated on the basis of previous experiences and on the recommendation of other neighbours.

E. Simulation setup

For simulation purposes, we will use MatLab 7.2. It is a most familiar tool for networking simulation purposes. We have explained about the simulation tools and method used in our paper for analyze of AODV and SS-AODV routing protocol performance. Performance metrics throughput, delay, latency, loss of packets, and byte-overhead are used for performance comparison of AODV and SS-AODV.

Table 1: Parameters for Simulation

Name of the Parameter	**Description**
Name of the Simulator	MatLab 7.2
Simulation Time	600s
Size of Mapping	800*800
Packet Size	512 bytes
Attack Type	Sinkhole Attack
Traffic Type	CBR
Number of nodes	50
Max Malicious nodes	16
Transmission Rate	5 Packets/sec
Transmission Range	250 m

F. Detecting malicious route containing Sinkhole

Here, to detect the sinkhole in the network, the proposed mechanism starts to find the number of hops on the second shortest route between two alternate nodes starting from the source. Here, in the condition that if number of hops in the second shortest path is greater than the predefined threshold, then it is indicated that a sinkhole is present in between the two nodes in the network. For example, the malicious path containing the closed sinkhole is:

SOURCE→A→B→F→DESTINATION

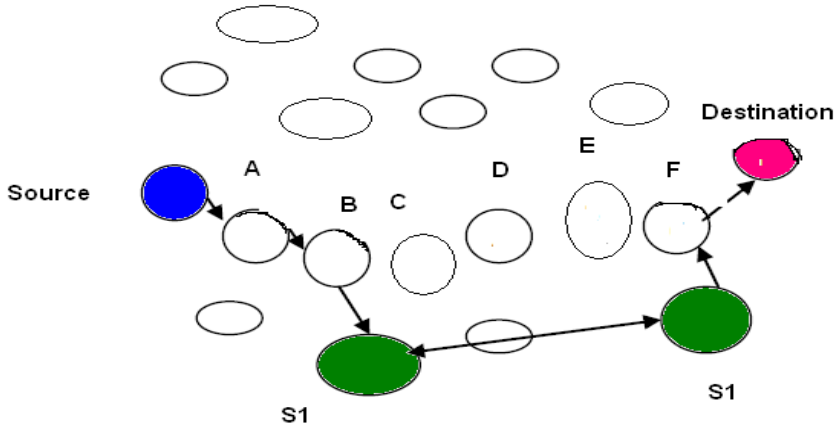

Fig. 3 Detecting Sinkhole Routing

IV. RESULTS DISCUSSION

AVERAGE THROUGHPUT**:** Average throughput means to how much data can be transferred from one node to another node in a given amount of time. It is generally measured in bits/second.

END TO END DELAY**:** End to End delay refers to that the time taken for a packet to be transmitted across a network from source to destination.

LATENCY**: Latency** is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses.

LOSS**:** Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss can be taken place by a number of factors including packet drop, corrupted packets rejected in-transit etc.

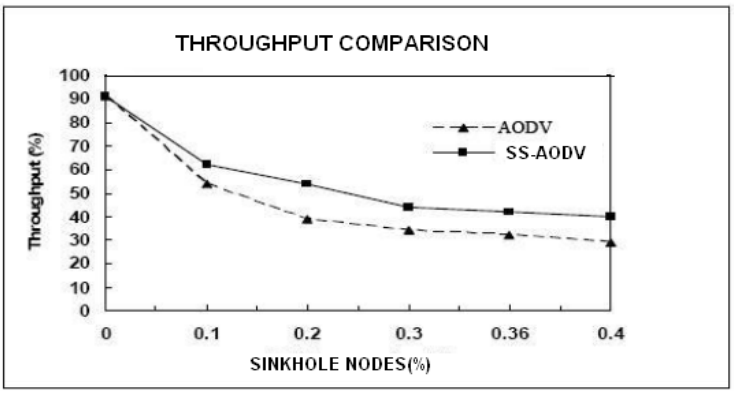

Fig. 4 Throughput comparison

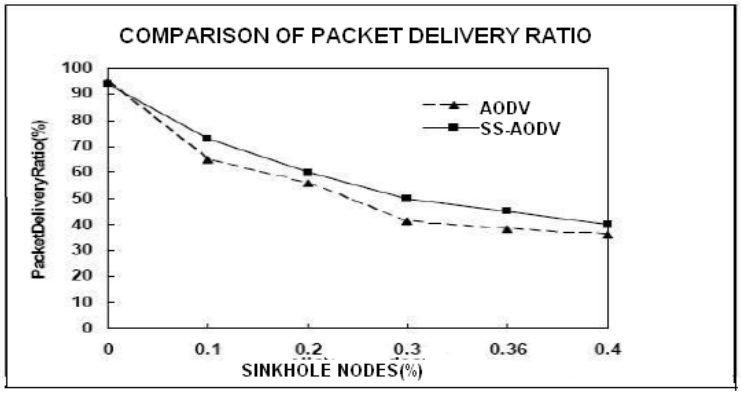

Fig.5 Packet delivery ratio

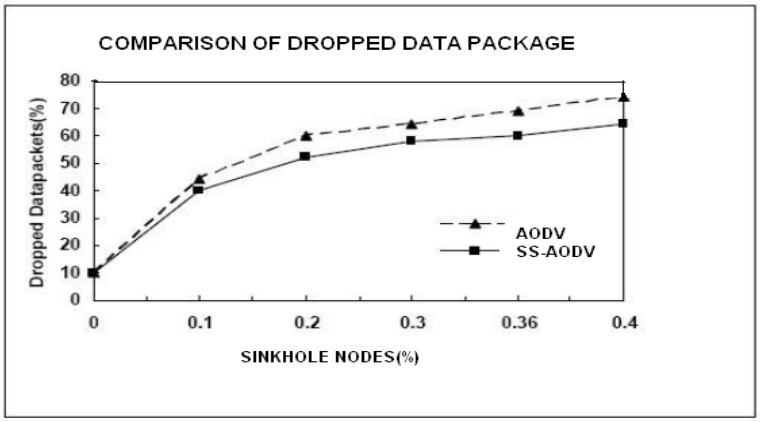

Fig. 6 Comparison of dropped data package

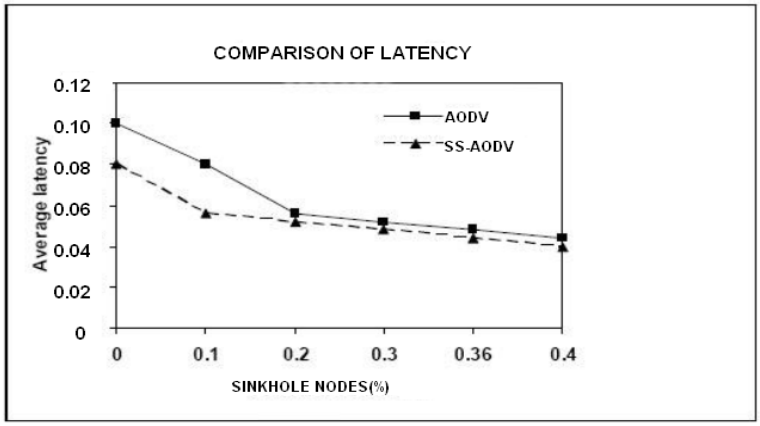

Fig. 7 Comparison of latency

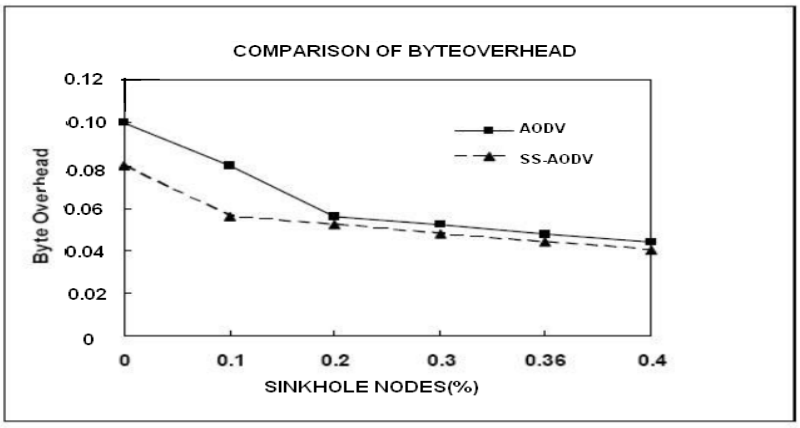

Fig. 8 Comparison of byte overhead

V. CONCLUSIONS

Wireless Mesh Network is very popular technology as compared to other existing wireless technologies. But this technology is vulnerable to various routing attacks. In this paper, we have proposed a secure routing scheme. By applying enhanced routing technique to detect sinkhole attack in WMNs, this technique uses routing variation between neighbours to find out the existence of a sinkhole. In this paper, we have presented a trust based approach through which association between nodes are used to resist sinkhole attack in WMNs. With the help of MATLab 7.24, we have represented that the proposed approach increases the secure routing and encourages the nodes to isolate the sinkhole nodes from the active data forwarding.

REFERENCES

[1] Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill Education Private Limited, 2010.
[2] A.Chinnasamy, S.Prakash, P.Selvakumari, "Enhance Trust based Routing Techniques against Sinkhole Attack in AODV based VANET", International Journal of Computer Applications (0975 – 8887) Volume 65– No.15, March 2013, pp 22-28.
[3] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model", IEEE transactions on network and service management, vol. 7, no. 3, september 2010, pp 172-176.
[4] www.wikipedia.org.

About the Author's

1. **Er. Pushpender** received the B.tech degree in Information Technology Engineering and M.Tech degree in Computer Science and Engineering from M.D. University, Rohtak (India). He has been in teaching profession more than three years. Beside he has the good industrial exposure in the field of computer technology and network. He is currently working as an Assistant Professor in the department of Computer Science and Engineering at S (PG) ITM, Rewari, India. Also he is a research scholar pursuing his Ph.D from Shri Venkateshwara University, Gajraula (UP), India in Wireless Mesh Network specializing Routing Protocols.

2. Dr. Sohan Garg: Presently working as **Director**, Sir Chhotu Ram Institute of Engineering and Technology, CCS University Campus Meerut, UP (India). He has worked as **Director**, IIMT Management College, Meerut, (UP), India. He received the Ph.D. degree in Computer Science from Institute of Advanced Studies, C.C.S. University Campus Meerut. He received the M.Tech degree in Computer Science from Manav *Bharti University, Shimla H.P (India).* He has published several research papers in National and international journals in his credit. He is also the guide of research scholar for almost twelve of Universities.

