ESWCRP: Efficient and Secure Weighted Cluster Routing Protocol-I

Basant Kumar Verma, Computer Science & Engineering, JSPM's Jayawant Institute of Computer Applications, Pune, India
Dr. Binod Kumar, Director, JSPM's Jayawant Institute of Computer Applications, Pune, India

ABSTRACT

In this paper, we are investigating the security of the wireless networks. As in different mobility based technologies the security and efficiency is a concern then need to address the key issues in network. In addition of that an effective solution is also need to be design. Therefore, in this paper the five goals are established (1) selection of appropriate routing protocol for implementation points of view (2) selection of routing based attack models and their impact on the network performance (3) designing of efficient weighted clustering based routing technique (4) improving security in weighted clustering algorithm (5) evaluation of the developed clustering based routing technique. Among these the first two objectives of the work are included in this paper. Additionally on the basis of experimental evaluation the AODV routing protocol is selected for implementation. Moreover it for demonstrating and finding solution for the security black-hole, wormhole, Gray-hole and DOS flooding attacks are considered. Finally paper concluded with the obtained network parameters that are helpful for identifying the different kinds of attack and their characterization.

Keywords

Wireless network, protocol comparison, attack analysis, security in wireless network

I. INTRODUCTION

The need of the communication and effective transmission of data is the main aim of computer networks. Therefore the wired technology is invented for the networking aspects. But the wired networks are increases the amount of installation cost, and maintenance cost. Therefore in the place of wired networks the wireless communication networks are adopted. This technology is becomes too much popular due to rapid installation, low cost and easy and low cost maintenance. The wireless communication is growing and providing ease in various kinds of applications additionally using the wireless communication concepts a number of different technology is also growing such as VANET (vehicular ad hoc networks) [1], WSN(wireless sensor networks) [2], WMN (wireless mesh networks) [3] and others.

In this work the wireless networks are investigated, basically the wireless network is a group of nodes which are form a network by connecting each other using wireless links. These nodes are either mobile or static based on the nature of application where the network employed. The nodes either works in static or in mobile some of resources are limited i.e. battery power, computational ability and others [4]. Therefore during the wireless network design the aim is to achieve high performance, where resources are utilized optimally. On the other hand when the network configured with mobility then it create a number of security as well as performance issues.

Therefore the mobile wireless networks are required to keep secure and efficient. But due to mobility a number of applications i.e. Environment Monitoring System [5], and Rehabilitation Applications [6] are getting benefits. Therefore the proposed work is intended to design and develop an efficient and secure technique by which both the primary concern of the network design are obtained.

II. OBJECTIVE

The proposed work is basically motivated from the concept of mobility in wireless sensor networks. A number of research articles on mobility based issues in wireless sensor network are published for performance [7] and security [8]. Additionally various articles for performance improvements [9], [10], [11] and security solutions [12], [13], [14], [15] are available. But most of the research is performed for individual security issues. But some of the solutions [16], [17] and [18] are motivates us for developing the entire network's security solutions. Therefore the weighted clustering algorithm based secure wireless network is proposed for solution formulation and research investigation.

The wireless networks are growing continuously and new techniques are developed to improve performance and security, but most of them either promise for higher

performance or for security. Thus a new technique is required that not only offers the efficient communication that promises to secure the entire network too. The proposed work is indented to develop a new Efficient and Secure Weighted Cluster Routing Protocol (ESWCRP). In order to develop such a routing protocol the following intermediate goals are established.

1. **To study the wireless network and obtain efficient routing protocol:** in this phase the wireless sensor network basics and applications are studied [19]. Additionally need to find different routing protocol for implementation and simulation points of view. A comparative study among different routing protocols is performed. This study provides an efficient routing protocol that is used for simulation and to develop efficient routing strategy.

2. **To secure the routing protocol and choose the attacks for simulation:** in this phase the different kinds of routing based attack is studied [19] and their impact on the routing performance is evaluated [20]. During this the some frequent attacks are concluded for simulation and solution development. Therefore the selected attacks are deployed and their effects on different performance parameters are studied. Finally solutions are also reviewed that are previously used for solution development.

3. **To improve the performance of wireless network:** in this phase the different kinds of routing protocol are developed for improving the performance of routing protocols. Additionally an improved routing protocol is proposed and implemented that enhance the performance of the network as compared to traditional routing protocols [21].

4. **To combine the security and performance in routing:** in this phase the efforts are made to combine the performance and security in wireless sensor network routing protocols. In addition of that an improved Efficient and Secure Weighted Cluster Routing Protocol (ESWCRP) is proposed and implemented that helps to achieve both the primary objectives (i.e. performance and security both).

5. **To evaluate performance of Efficient and Secure Weighted Cluster Routing Protocol (ESWCRP):** in this phase the proposed routing protocol is evaluated on various performance parameters and their results are discussed for different security constraints and performance.

III. ASSUMPTION AND DEPENDENCIES

In order to prepare a secure and efficient routing for the wireless sensor network the following assumptions are made.

A. Network assumption

The wireless sensor network is assumed as a group of nodes connected with the wireless connectivity. Additionally that is developed with the limited power source, and computational ability. The network can support the both kinds of topology static or dynamic, for experimentation purpose here dynamic topology of network is considered. The dynamic topology of network can able to adopt new nodes for communication during route discovery process. The network simulation is prepared using network simulator NS2 version 2.35 environment. The different network simulation and performance analysis is conducted over 20, 40, 60, 80 and 100 sensor nodes.

B. Security assumptions

Due to ad hoc and random mobility of wireless sensor nodes the topology is created dynamically. The topology creation needs a route discovery process for preparing the route among two communicating nodes. Therefore, the malicious node can also join the network and actively participate for accessing the services distributed by the network at a point of time. Therefore the attacker node can use the routing information for deploying attack. Therefore the routing based attacks are considered in this work. A number of attacks can be deployed using the routing information therefore for simulation and performance evaluation of the proposed security solution the wormhole, Gray-hole, Black-hole and DDOS attacks are considered.

IV. SELECTION OF ROUTING PROTOCOL

This section describes the key features of different routing protocols that are supporting the Mobile network such as DSDV, DSR, and AODV. That also describes the particular parameters that are used for implementing proposed routing protocol.

A. Destination-Sequenced Distance Vector (DSDV)

DSDV is known as Destination-Sequenced Distance-Vector Routing protocol. That is a table-driven routing for mobile ad hoc networks. That is derived with the help of Bellman-Ford algorithm. That is loop free protocol by including sequence numbers. In DSDV protocol each node has a routing table. An entry of the table encloses the

address identifier, shortest known diffidence metric. The distance measured in hop counts and address identifier of node is the first hop on routing table. A routing table has all destinations and number of hops in network. A sequence number is associated with each path to the destination. The route with highest sequence number is used. Moreover it helps to know the fresh routes, and to avoid formation of loops in path. Additionally to minimize traffic, the two types of packets are used. First packet finds the route change. Second packet called "incremental" that will carry just the changes. This concept helps to grow overall network capability. DSDV is a regular update based protocol need to update its routing tables in a defined period of time. Due to this a considerable amount of battery power and bandwidth is consumed. As network topology changes new sequence number required before re-organization of network [22].

B. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is based on a design known as resource routing. It is equivalent to AODV because it forms a route on-demand. Excluding that, every intermediate node that forward RREQ packet adds its own address identifier. The destination node produce RREP that comprise the list of addresses received in route and broadcast it to create reserve path. Route maintenance in DSR is accomplished by acknowledgements (ACK). These replays can be link-layer ACK, passive ACK or network-layer ACK produces by DSR protocol. It uses resources routing instead of relying on the routing table at each in-between device. When a node is not acknowledges the successful reception of a packet it tries to retransmit it. While a finite number of retransmissions fail, the node produce route error message that recognize the broken link.

When a node wants a route, which it doesn't have in its route cache, it broadcast a RREQ message. Every RREQ packet is recognized by initiator's address and observance id. RREQ is replied by destination node, which differentiate route, using RREP message. The reverse route for RREP message is one of the routes that live in the route cache (if it exists) or a list concerning turn of the nodes in the RREQ packet if common routing is supported. The routes are possibly unidirectional or bidirectional. DSR doesn't use of periodic messages from the hosts for preservation of routes. It uses two kinds of packets for routes: Route Error (RERR) and ACKs. When, a node finds broadcast errors so source receives a RERR message. ACK packets are used to bear out the correct procedure of the route links [23].

C. AODV routing

The routing protocols DSR and DSDV are hybridized for developing AODV protocol. The Route Discovery and Route Maintenance properties are taken from DSR and relay process or hop-by-hop routing, sequence numbers, and periodic information exchange is inherited from DSDV [24].

To understand process of AODV supposes a node S wants to send some data to a node D. So, node S broad-casts a RREQ message to its neighbors, with the last sequence number. The RREQ is flooded in a regulated fashion by which packet is used to create a path between S and D. Thus each intermediate node forwards RREQ towards destination and an additional route to itself in reverse manner to node S. When RREQ reaches to D, the destination node D creates a RREP message. That packet contains number of hops to D and sequence number for D. All nodes that participates in forwarding RREP back to source using RREQ, creates a forward route to D. The similar process is used to prepare a path between S to D. Therefore the entire node only sends or receives data for a single hop, not for the whole route.

To keep routes, AODV need that each node often broadcast a Hello message in a default rate. When three successive Hello packets are not received then recognized as link failure. Otherwise, AODV use link layer to recognize link failure [25].When a route become fails upstream nodes are notified by an Unsolicited Route Reply. The recipient of such a REPLY concludes that a node becomes fail and need to discover a new route.

D. Comparative Performance Study

This section provides performance analysis of the studied routing protocols. On the basis of the performance an efficient routing is selected. That supports small as well as large network efficiently with less resource consumption. Therefore a simulation using NS2 simulator is performed and with increasing traffic.

a. Packet delivery ratio

The packet delivery ratio is prerogative number of received packets by principle node to number of packets sent by all the nodes. The comparative PDR of the DSDV, AODV and DSR protocols are given in figure 1 with growing network size. The X axis contains number of nodes and percentage of delivered packets is given in Y axis. The blue line shows performance of DSDV, red line represents AODV and green line is used for DSR protocol. According to results performance of DSR protocol is adoptable as compared to DSDV and AODV protocols. But DSR is not suitable to serve the large network because of the slow processing and large size of routing table. Consequently the appearance in diminishing order can be DSDV→AODV → DSR.

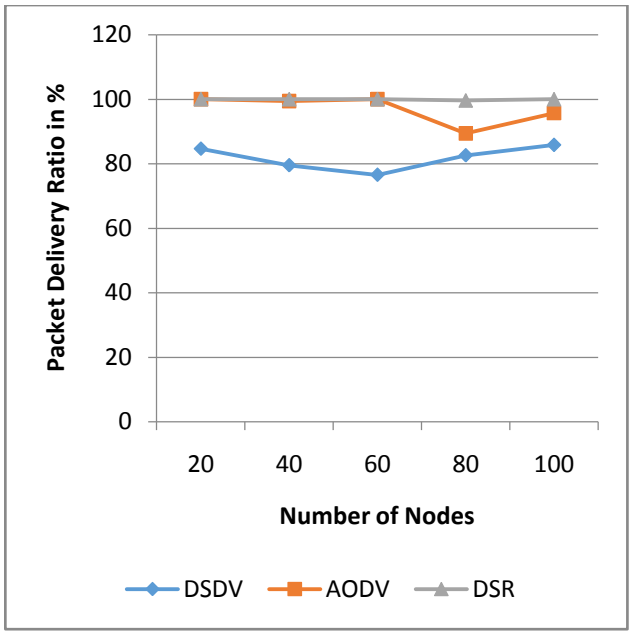

Figure 1 Packet delivery ratio

b. Routing Overheads

Routing overheads is the number of control packets produce by every routing protocol through reproduction. It is the internal determine or competence any routing protocols. Two dissimilar routing protocols can use dissimilar amounts of overheads depending on their internal capability. If control and data traffic share the similar channel and channel ability is limited then extreme control traffic frequently impacts data routing presentation (throughput). If more control packets are sent by the routing agents, then delay in the network will also increase. The comparative routing overhead of the routing protocols with increasing size of traffic is given using figure 2. In this diagram the amount of transparency is symbolize using Y axis and the number of nodes are listed in X axis. According to the obtain results the external of DSR routing procedure is a great deal higher than the DSDV and DSR routing in situation of routing simplicity. Therefore DSR is additional adoptable for mobile ad hoc network routing.

c. Remain Energy

The amount of energy preserved during the active sessions of communication is known as remain energy. The ad hoc devices are occupied throughout the inbuilt energy reserve therefore for every incidence in network a fixed amount of energy is compulsive from the initial energy. Figure 3 shows the amount of remain energy in dissimilar routing sessions over growing traffic size. The amount of comparative energy consumption is given using figure 3 in this diagram the percentage amount of energy consumption is given in Y axis and the X axis contains the number of nodes in network.

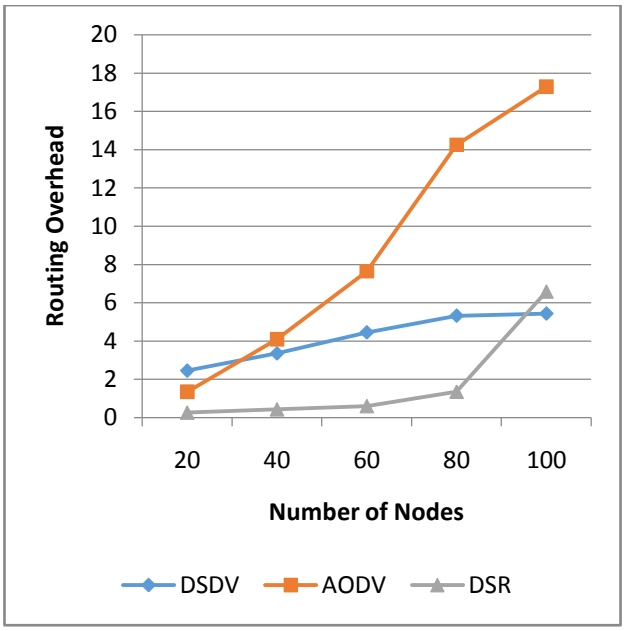

Figure 2 Routing overhead

According to the evaluated results of the energy consumption the DSR routing consumes more energy as compared to the DSDV and AODV routing protocol. Notice that according to the MANET property low battery can concern the network functioning therefore the DSR is not successful for the long reproduction moreover the DSR is not much acceptable for the big network for reproduction of DSR the amount of associations are very less as compared to previous two routing protocols.

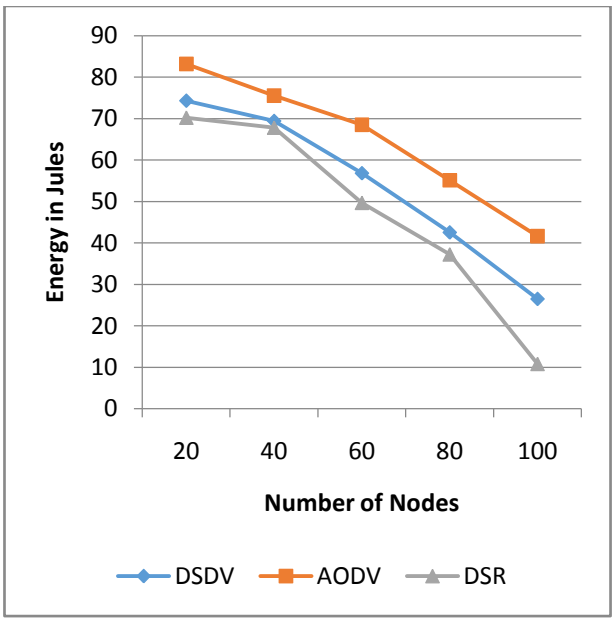

Figure 3 energy consumption

E. Discussions on Results

This chapter provides the brief study of the wireless communication network and the different variants of wireless networks. In further discussion the mobile ad hoc network is discussed in detail. In this chapter that is known the key component of the entire network functioning is depends on the routing strategy. Consequently dissimilar routing protocols are discussed additional specifically OLSR, DSR, DSDV and AODV routing protocols. Finally for performance improvement of the mobile ad hoc network the clustering approaches are discussed. In order to acquire the resourceful and responsible communication for little and big networks the presentation study made amongst the AODV, DSDV and DSR routing protocols.

The comparisons of the routing protocols are performed in terms of energy consumption, routing overhead and the packet delivery ratio. Additionally to compare them the performance is evaluated under different number of nodes in network (i.e.20, 40, 60, 80 and 100). After experiments a mean performance is also computed for clarifying the performance of compared routing protocols. For computing the mean performance the following formula is used:

$$Mean\ Performance = \frac{1}{N}\sum_{i=1}^{N} Obtained\ results_i$$

Where N is the number of experimental observations made over different number of nodes.

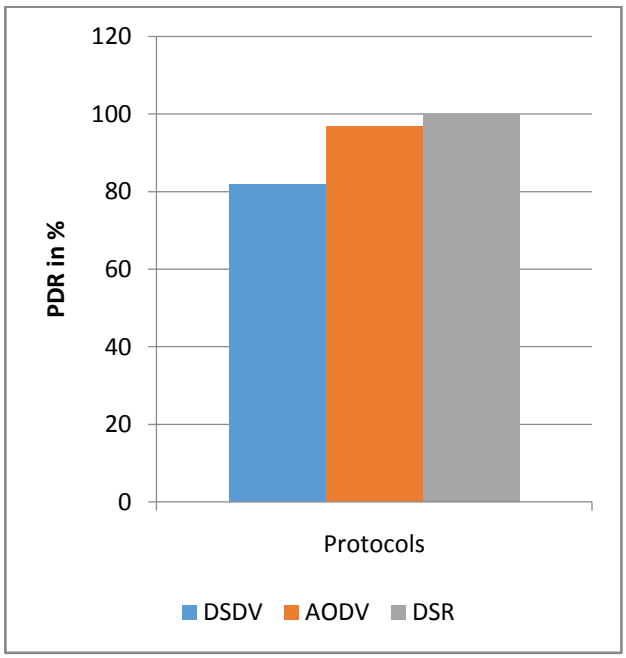

Figure 4 Mean packet delivery ratio

The obtained performance in terms of mean packet delivery ratio is demonstrated using figure 4.

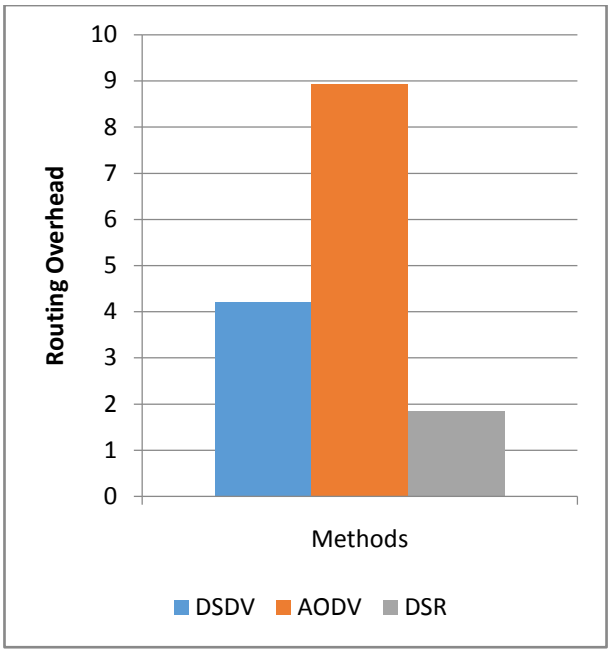

Figure 5 Mean routing overhead

In this diagram the implemented protocols are given in X axis and the Y axis shows the obtained mean packet delivery ratio in terms of percentage (%). To represent the performance blue lines are used for DSDV routing protocol, red line shows AODV and the green line demonstrate DSR routing performance. According to the obtained results the performance of DSR routing protocol is much efficient as compared to both the routing protocols. In the similar manner the performance of routing protocols (AODV, DSDV and DSR) are compared in terms of mean routing overhead using figure 5. In this diagram the routing overheads of the tree implemented protocols are demonstrated. According to the figure 5 the performance of DSDV is defined using blue line, the AODV is simulated using red line and the DSR routing is given using figure green line. In this diagram the X axis contains the different number of nodes and the Y axis shows the routing overhead of the protocols. According to the outcomes DSR produces less routing overhead as compared to both the routing protocols. Similarly the mean energy consumption is demonstrated in figure 6. In this diagram the X axis shows the protocols implemented and Y axis shows remaining energy of node. According to the outcomes the AODV routing protocol preserves more energy as compared to both the protocols. Thus AODV routing is comparatively efficient algorithm.

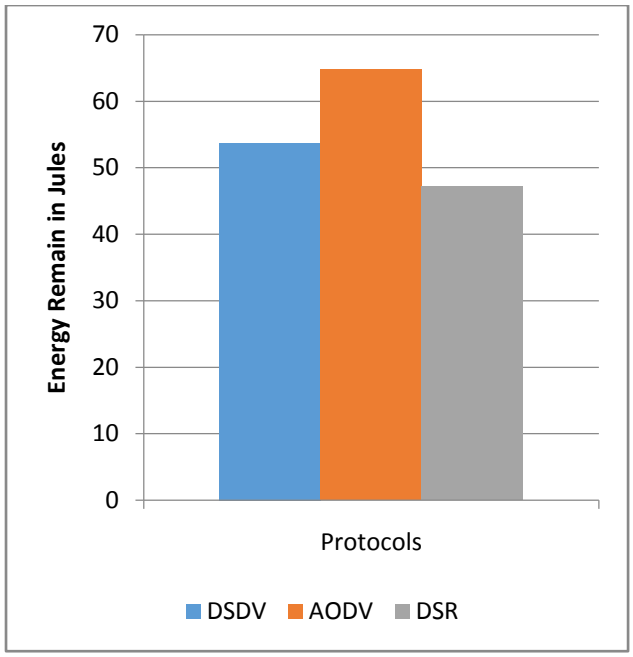

Figure 6 Mean energy consumption

In the comparisons of these routing protocols the AODV routing protocol is found mainly consistent routing technology since of this is much elastic to support small networks as well big networks. In adding of that in previous presentation parameters such as packet delivery ratio, throughput and the end to end delay the DSR routing protocol are much efficient then the AODV routing protocol. But the AODV routing protocol is energy save technology too, since of the less control message substitute and less episodic message relations. Behind that the AODV routing is obtained as the mainly optimum routing procedure for the residual experimentations.

V. ATTACK MODELS

The given section introduces the different attacks which are selected for the experimental evaluation with the proposed secure network in the ad hoc mobility scenarios.

A. Black-hole Attack

A black hole attack [26] is a type of DOS attack that can be easily employed against routing in Ad-hoc networks. In this attack, a malicious node tries to attract all network packets by advertise itself as having the shortest path. When attacker node receives, an RREQ message, it instantly sends a false RREP message. Consequently source node supposes that route detection procedure is finished and ignores other RREP messages and begins to send packets to attacker node. Attacker node attacks all RREQ messages this way and takes over all routes. Consequently all packets are sent to a path are dropped and will not be reached to appropriate destination.

B. Wormhole Attack

In wormhole attack a node receives packets at one location in network and sends it to a different location. The wormhole link is established between two or more nodes for sending data packet and it could be established via wired link or wireless link between two attackers. When node transfer data via wormhole link than attacker are able to gain the confidential information, or drop the packet [27].Figure 7 shows an example of the wormhole. A1 and A2 are two attackers that are connected by high speed channel. When source S wand to send a packet to destination D than it send a RREQ packet for finding a route between source to destination. S sends a RREQ packet to its immediate neighbors J and K, J and K receive a packet and send it to their neighbors. And node A1 which is the neighbor of J when Received the RREQ packet than it send a RREQ packet to malicious node A2 via high speed channel, A2 rebroadcast the RREQ to its neighbor P, request which passes through a wormhole link reach at destination first because colluding node are connected through high speed channel. So D will choose route and send a RREP via a path D-P-J-S and ignore the other RREQ that arrive later. Then S sends a data packet via a path S-J-P-D to destination D.

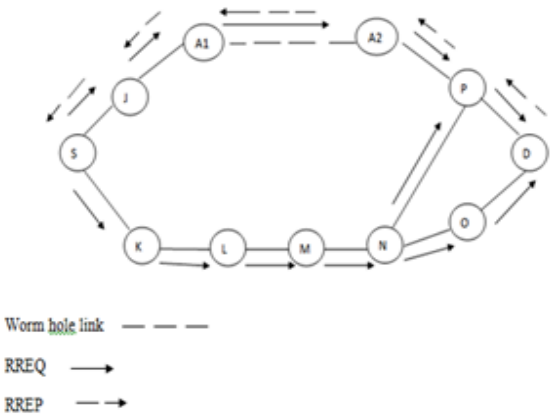

Figure 7 Wormhole Attack

Deployment of Wormhole Attack

Tunnel can be established between nodes by Packet Encapsulation, out of band hidden channel and high transmission power [28].

- **Wormhole using Packet Encapsulation:** This method work in hidden mode. Several nodes exist between two malicious nodes and data packets are encapsulated between malicious nodes. Hence it prevents nodes from incrementing hop counts. The

packet is converted into original form by the second end point.

- **Wormhole using high power transmission:** It can launch by single malicious node which has a high transmission capability to attract the traffic, so legitimate nodes choose a path that contain malicious node for transfer the packet. The chances of malicious nodes present in the routes established between sender and destination node.

- **Wormhole using Packet Relay:** One or more malicious nodes can launch packet-relay-based wormhole attacks. In this type of attack malicious node deliver data packets between two distant nodes and this way it creates illusion that two nodes are neighbor.

- **Wormhole using Protocol Distortion:** In this type, single malicious node attract traffic for passing through it by distorting protocol rule, like nodes have to wait for sometimes before retransmitting. But malicious nodes don't follow this rule and retransmitted a packet again and again so it could reach to the destination first, Even if any request reaches the destination later. They will be dropped by destination.

- **Wormhole using out of band:** This two ended wormhole, a dedicated high bandwidth channel between two end points to form wormhole link [29].

Types of Wormhole Attack

Wormhole attacks are classified using different criteria based upon:

***Classification based upon Implementation*:** Based upon implementation, wormhole attacks can be classified into the following types.

- **Using Encapsulation:** There a several node exist b/w malicious node, in this type of mode separate tunnel doesn't establish b/w malicious node, and packet is transferred by normal path, Here attacker hide themselves in routing path means source doesn't know that malicious node present in routing path.

- **Using out-of-band channel:** It uses an out of band channel b\w malicious nodes. This channel can be established by a long range wireless link or a wired link. This type of attack is very challenging to launch and it required specialized hardware to deploy. Regard as the situation depicted in Figure 8.

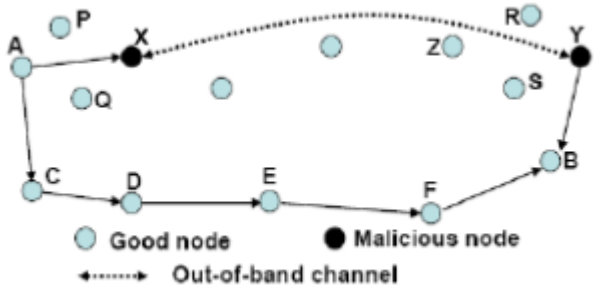

Figure 8 Wormhole Attack Using Out Of Band Channel

Node A sends a RREQ to node B, and nodes X and Y are malicious nodes include an out-of-band channel between them. Node X tunnels the RREQ to Y, Node Y transmit the packet to its neighbors B. B gets two RREQs—A-X-Y-B and A-C-D-E-F-B. The first RREQ has lesser hop count than second one so it is chosen by B.

Classification based upon Medium Used:

Wormhole attacks can be also classified as In-Band and Out-of-Band wormhole attacks.

- **In-band wormhole:** This attack launch in hidden mode. Attackers are using following methods for creating link between them e.g. Encapsulation, Packet relay and Protocol deviations.

- **Out-Of-Band Wormhole:** This attack launch in participation mode. Attackers are using following method to create a link between them e.g. Out-Of-Band Channel and High Transmission Mode [30] [31].

Classification based upon Attackers:

- **Self-Sufficient:** Where colluders advertise themselves as normal nodes, all paths passes through them e.g. out-of-band channel or using high power transmission. Our approach focuses on detection of such type of wormhole nodes and attacks.

- **Extended Wormhole:** The colluders are hidden by themselves and extend the attacks beyond themselves to normal nodes e.g. encapsulation or packets relay [30].

Classification based upon location of Victim nodes.

- **Simplex:** Targeted node lies in range of only one attacker.

- **Duplex:** Targeted node lies in range of both the attackers [30].

Another type of Wormhole Attack

There are three types of wormhole attack closed, half open, and open. In which S and D are the source and destination nodes respectively. Nodes M1 and M2 are malicious nodes.

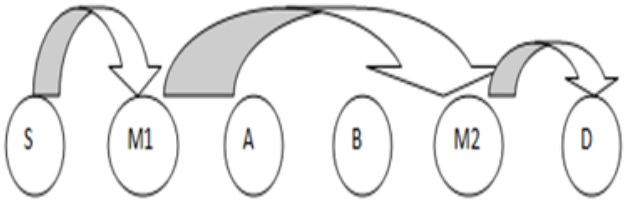

Figure 9 Open Wormhole

Open Wormhole: In this type of attack both malicious node M1 and M2 are visible, nodes aware about the presence of malicious node, in this malicious node doesn't hide themselves in RREQ packet header [31]. Consider the scenario depicted in figure 9. Node M1 and M2 are visible and nodes A and B that exist between Malicious nodes M1 and M2 are kept hidden, so source(S) sends packet to destination(D) via the path S-M1-M2-D

Half-Open Wormhole: In this one side of malicious node is hidden and other side of node is visible [32].In this route discovery procedure, malicious node M1 is visible, although second node M2 is kept hidden, and node between M1 and M2 is also kept hidden. So packet is sent via path S-M1-D, Malicious nodes don't modify the content of packet they simply tunnel them from one location to other location [32].

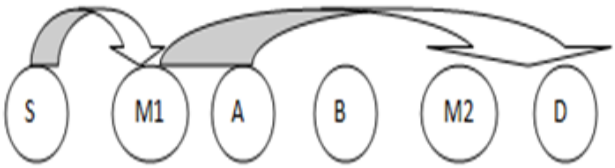

Figure 10 half open Wormhole

Close Wormhole: In this type of attack both malicious node M1 and M2 and the nodes exist between M1 and M2 are kept hidden. In this both source and destination node assume that they are direct neighbor .The attackers do not transform the content of the packet. Just, they basically move the packet form one side of wormhole to a further side and it rebroadcasts the packet [32].

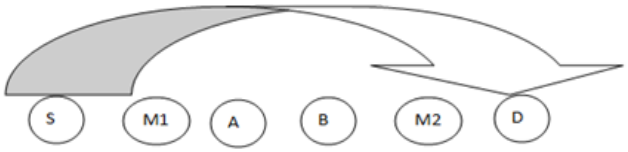

Figure 11 Close Wormhole Attack

C. Gray-hole Attack

In this kind of attack the attacker misleads the network by approving to forward the packets. As it receives the packets from neighbor node, attacker fall the packets. This is a type of active attack. In beginning attacker nodes behaves usually and reply true RREP messages to nodes that started RREQ messages. When it receives data packets it starts falling packets and launch Denial of Service (DOS) attack. The malicious activities of Gray-hole attack are different in different ways. It drops packets while forwarding them in the network. In some other Gray-hole attacks attacker node behaves maliciously for time until packets are dropped and then switch to their normal behavior. Due this it's very tricky for the network to figure out such kind of attack. Gray-hole attack is also termed as node misbehaving attack [33].

D. DDOS Attack

A common technique of attack involves saturating the target machine with communications requests, by which target machine cannot respond to legitimate traffic, or responds slowly. In other terms, DDOS attacks are deployed by forcing the targeted machine to reset or consuming its resources by which that machine no longer provide its services. There are two chief classes of DDOS attacks: bandwidth depletion and resource depletion attacks [34].

1. **Bandwidth depletion:** Bandwidth depletion attack is designed to flood the victim network with unwanted traffic by sending that stops legitimate traffic from reaching the victim system. Bandwidth attacks can be separated to flood attacks and amplification attacks.

2. **Resource depletion:** Resource depletion attack is an attack that is planned to tie up the resources of a victim system. This is done by developing the TCP protocol and sending will fully incorrect semantic IP packets to crash the victim system. This type of attack can be separated to protocol exploit attacks and malformed packet attacks.

E. Experimental setup

In order to measure the impact of different attack in the wireless sensor network, the experimental environment is created in NS2 simulation. In order to simulate the effect of the different attack following simulation parameters are setting up shown in table 1.

Table 1 Simulation Setup

Simulation properties	Values
Antenna model	Omni Antenna
Dimension	1000 X 1000
Radio-propagation	Two Ray Ground
CBR Packet Size	512 Bytes
Interface Queue Length	50
Channel Type	Wireless Channel
No of Mobile Nodes	20
Interface Queue	Droptail/ Priority Queue
Link Layer	LL
Routing protocol	AODV
Time of simulation	60.0 Sec.

F. Experimental attack analysis

In order to characterize the effect of considered attacks the following scenario are desired to implement for simulation.

a. Simulation of Black-hole Attack

Black-hole attack basically deployed using the intermediate router which populates self as the shortest route among the available routes from source to destination. Thus, when the source routers get the information of shortest route and send data through it than most of the data is dropped by this node. According to the evaluated outcomes in terms of the Packet Delivery Ratio and Remain Energy during the Black-hole node deployment is given using figure 12 and 13. In this experimentation the network is configured using the AODV routing protocol and the simulation is performed in normal conditions for 60 seconds. The performance under simple AODV configuration is given using green line. At the same time with the similar configuration of network a Black-hole attacker is introduced in network and then again performance is estimated which is demonstrated using red line.

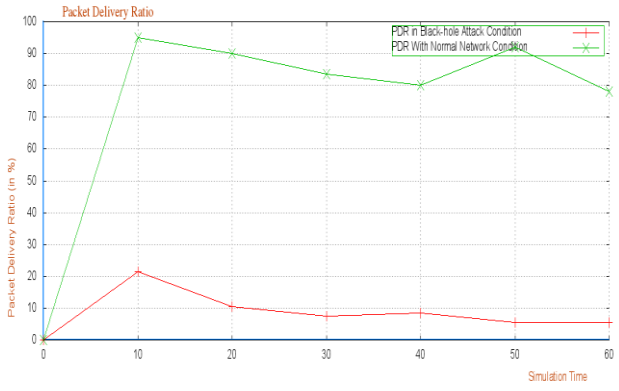

Figure 12 PDR vs Simulation Time (Black-hole)

In the figure 12, the X axis shows the simulation time and the Y axis shows the percentage of packet delivery ratio. According to the results the packet delivery ratio is significantly reduced at the time of Black-hole node deployment. Similarly in figure 13, the X axis shows the simulation time and the Y axis shows the energy remained. According to the obtain results the energy is significantly reduced at the time Black-hole node deployment. The results are also summarized for 20-nodes as given in table 2, which represents the comparison of the Packet Delivery Ratio and Remain Energy under Normal network condition and Black-hole attack condition.

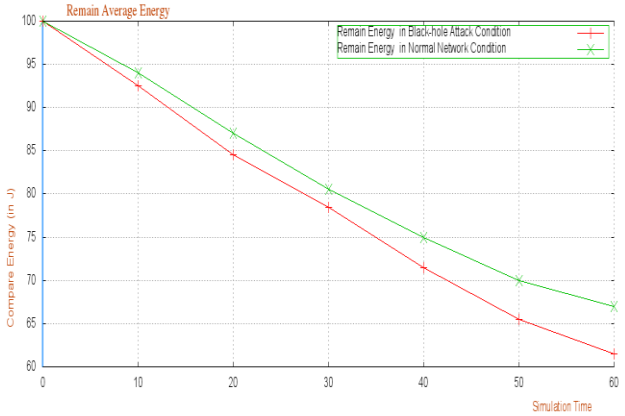

Figure 13 Energy vs Simulation Time (Black-hole)

Table 2 Comparisons under Normal Network and Black-hole Attack

Performance Metrics	Normal Network	Black-hole Attack
Packet Delivery Ratio	Maximum	Minimum
Remain Energy	Highest	Lowest

b. Simulation of Denial of Service Attack

Denial of Service Attack is a kind of resource consumption attack, during this attack deployment the malicious node tries to communicate with most of the neighbor nodes. Thus the bandwidth consumption, energy consumption and the drop ratio of network increases that is shown in figure 14, 15 and 16. Figure 14 shows the connectivity request with respect to the time of simulation therefore during normal conditions the network behavior in terms of connection request is simulated using green line which shows the limited number of request send during communication sessions. On the other hand, the amount of increasing connection request as shown using red line which demonstrates the number of connection requests sends by the malicious node's behavior. Similarly, Figure 15 and 16 shows the performance of network under DOS attack in terms of packet deliver ratio

and remain energy. According to the obtained results the packet delivery ratio and energy is also significantly reduced when the DOS attack is deployed in network. The results are also summarized for 20-nodes as given in table 3, which represents the comparison of the Packet Delivery Ratio, Route Requests and Remain Energy under Normal network condition and DOS attack condition.

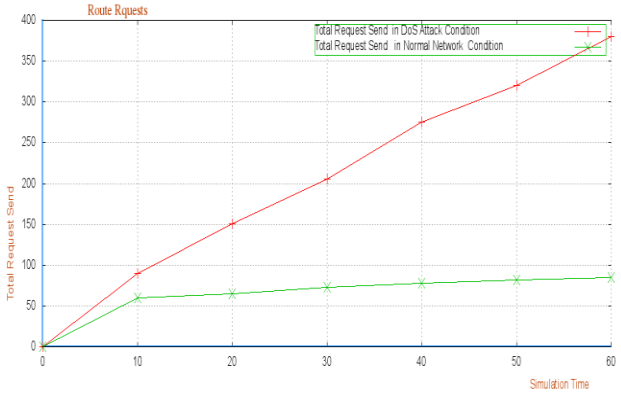

Figure 14 Route Request vs Simulation Time (DOS)

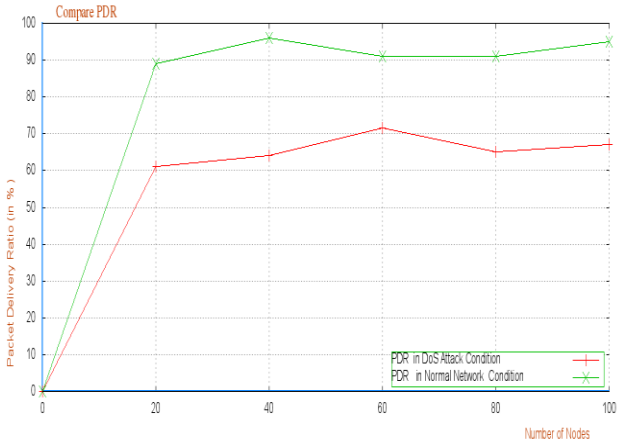

Figure 15 PDR vs Simulation Time (DOS)

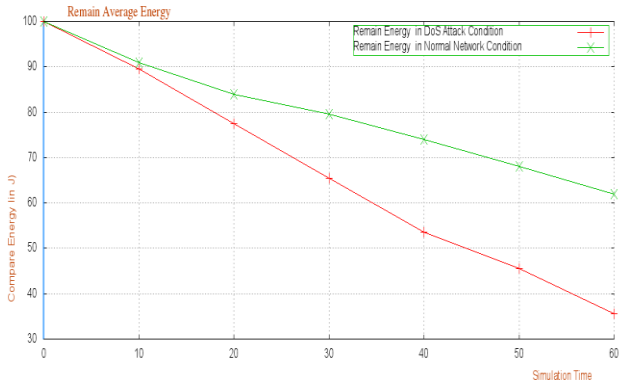

Figure 16 Energy vs Simulation Time (DOS)

Table 3 Comparisons under Normal Network and DOS Attack

Performance Metrics	Normal Network	DOS Attack
No. of Connection Request Send	Minimum	Maximum
Packet Delivery Ratio	Maximum	Minimum
Remain Energy	Maximum	Minimum

c. Simulation of Gray-Hole Attack

The Gray-hole attack is a variant of Black-hole attack. The only difference is that the Black-hole attacker drops all the packets but during the Gray-hole attack only selected packets are dropped. Due to attacker's selective forwarding methodology of data manipulation the network is not much aware about the attacker and simulating the normal functionality. In order to understand the given phenomena the simulation of Gray-hole attack is performed with the help of AODV routing protocol for 60 second. The performance outcomes under the Gray-hole attack is given using figure 17 and 18 which shows the performance of packet delivery ratio and remain energy under Gray-hole attack condition and Normal network condition.

Figure 17 PDR vs Simulation Time (Gray-hole)

The figure 17 shows the performance of network during the normal conditions using green line and under the Gray-hole attack using red line. During Normal network conditions the network is able to deliver packets more efficiently and on average packet delivery ratio is found between 80-100%. On the other hand the performance of the network is reduces about half of the actual performance of network in Gray-hole attack condition. Therefore during attack the performance in terms of packet delivery ratio is found between 39-60%. Similarly in figure 18, remains energy also reduced when the Gray-hole attack is deployed in the network. The results are also summarized for 20-nodes as given in table 4, which represents the comparison of the Packet Delivery Ratio

and Remain Energy under Normal network condition and Worm-hole attack condition.

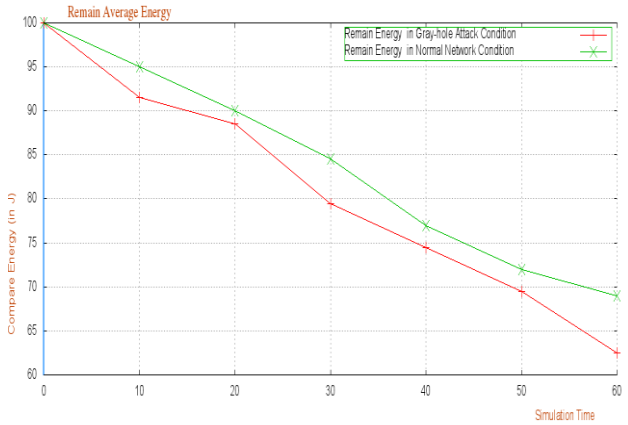

Figure 4.20 Energy vs Simulation Time (Gray-hole)

Table 4 Comparison under Normal Network and Gray-hole Attack

Performance Metrics	Normal Network	Gray-hole Attack
Packet Delivery Ratio	Maximum	Minimum
Remain Energy	Highest	Lowest

d. Simulation under Wormhole Attack

Wormhole attack is also deployed using the intermediate routers in network routes, in this kind of attack more than two attackers join the network. All the attacker nodes are connected through the high speed data buses or direct efficient links.

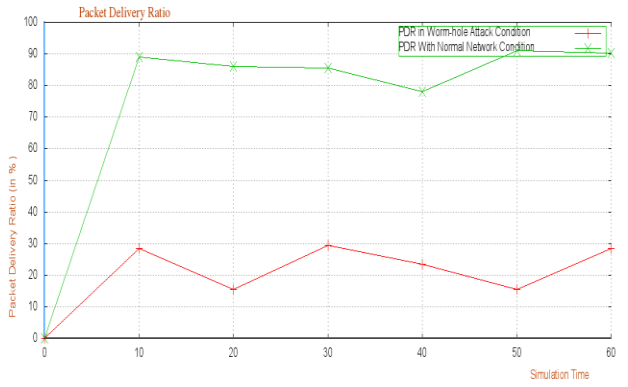

Figure 19 PDR vs Simulation Time (Wormhole)

These nodes are also advertising self for having the shortest route or optimal route. When they found the data packets then they misguide the data in route or drop the collected data. That as shown using figures 19 where the packet delivery ratio of network is simulated. According to the simulated results during the normal conditions the network is working efficiently and during attack conditions the packets are dropped much rapidly. In addition of that with packet delivery ratio the network Round Trip Time (RTT) and energy consumption also increases in significant amount. This effect is simulated using given figure 20 and 21.

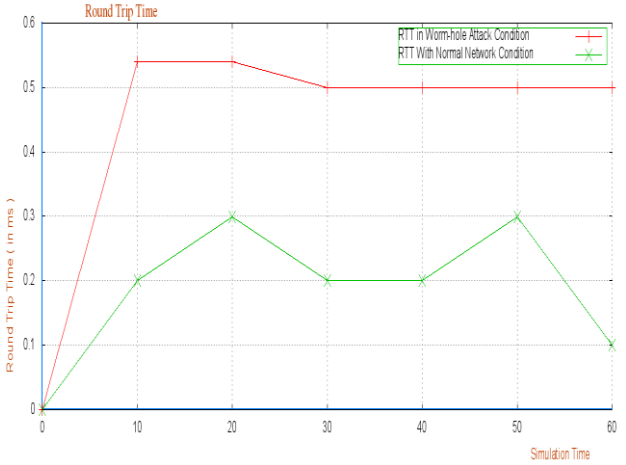

Figure 20 RTT vs Simulation Time (Wormhole)

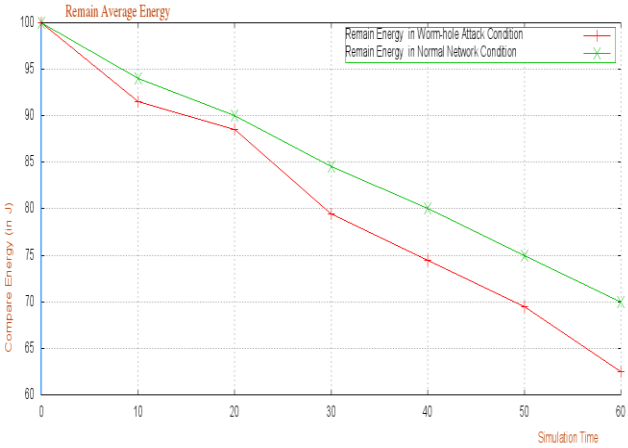

Figure 21 Energy vs Simulation Time (Wormhole)

In figure 20 the RTT is found normal in the normal condition and during attack condition RTT having higher values as compared to normal conditions. Similarly in figure 21 the remain energy is found maximum in the normal condition and during attack condition energy level is minimum as compared to normal conditions. The results are also summarized for 20-nodes as given in table 5, which represents the comparison of the Packet Delivery Ratio and Round Trip Time under Normal network condition and Worm-hole attack condition.

Table 5 Comparison under Normal Network and Worm-hole Attack

Performance Metrics	Normal Network	Worm-hole Attack
Packet Delivery Ratio	Maximum	Minimum
Round Trip Time	Minimum	Maximum
Remain Energy	Highest	Lowest

VI. CONCLUSION

In mobile wireless network the network devices are connected using wireless links. The connection among devices depends on radio strength they receive from neighbor nodes. Due to mobility network device changes their places frequently and connectivity among entire devices never remain constant. Thus, the network any time adopts new nodes and any node can leave network. Additionally most of security flaws are occurred due to this phenomenon too. This paper includes the detailed investigation of first two objectives established for the study thus first the different routing protocols are compared and four different routing based attacks are used for experimentation. Finally, the frequently deployable security attacks are selected namely Black-hole, Denial of Service, Gray-hole and Worm-hole for the network characteristics analysis.

To obtain different attack characteristics simulation study is performed with AODV protocol. During this simulation DOS flooding attack, Black-hole attack, Worm-hole attack and the Gray-hole attack is simulated and their effect on network performance is evaluated. According to the evaluated results, it is found that the DOS attack is a kind of resource consumption attack. Therefore during this attack the network resources are consumed frequently. On the other hand, the network performance in terms of packet delivery ratio and energy is degraded considerably during Worm-hole, Black-hole and Gray-hole attack. During this study, it is also recognized that buffer length, propagation time, remain energy and the packet delivery ratio are the most essential network parameters by which the attack conditions are recognized in network.

In the next part of the paper the detailed security system design and the performance improvement of security algorithm is performed with their results evaluation.

REFERENCES

[1] SalehYousefi, Mahmoud SiadatMousavi and MahmoodFathy, “Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives”, 6th International Conference on ITS Telecommunications Proceedings, 2006.

[2] Jennifer Yick, Biswanath Mukherjee and DipakGhosal, “Wireless sensor network survey”, Computer Networks, Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 52, PP. 2292-2330, August, 2008.

[3] AshishRaniwala and Tzi-ckerChiueh, “Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network”, In Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 2005.

[4] Shio Kumar Singh, M P Singh, and D K Singh, “Routing Protocols in Wireless Sensor Networks – A Survey”, International Journal of Computer Science & Engineering Survey (IJCSES) Volume 1, No.2, November 2010.

[5] MohdFauzi Othman, KhairunnisaShazali, “Wireless Sensor Network Applications: A Study in Environment Monitoring System”, International Symposium on Robotics and Intelligent Sensors (IRIS 2012),PP. 1204 – 1210, Volume 41, 2012.

[6] AbdelkrimHadjidj, Marion Souil, Abdelmadjid Bouabdallah, Yacine Challal, Henry Owen, “Wireless Sensor Networks for Rehabilitation Applications: Challenges and Opportunities”, Journal of Network and Computer Applications, Elsevier, Volume 36, PP.1-15, 2013.

[7] You-Chiun Wang, Fang-Jing Wu and Yu-Chee Tseng, “Mobility management algorithms and applications for mobile sensor networks”, Wireless Communications and Mobile Computing, PP. 7-21, 2012.

[8] Guangjie Han, Jinfang Jiang, and Han-Chieh Chao, “Management and applications of trust in Wireless Sensor Networks: A survey”, Journal of Computer and System Sciences, Volume 80, PP. 602-617 2014.

[9] AdamuMurtalaZungeru, KahPhooiSeng, and Wai Chong Chia, “Energy Efficiency Performance Improvements for Ant-Based Routing Algorithm in Wireless Sensor Networks”, Hindawi Publishing Corporation Journal of Sensors, Volume 2013, 17 pages, Year 2013.

[10] Mo Li, Zhenjiang Li, and Athanasios V. Vasilakos, “A Survey on Topology Control in Wireless Sensor Networks: Taxonomy, Comparative Study, and

Open Issues", Proceedings of the IEEE, Volume 101, No. 12, PP. 2538 – 2557, December 2013.

[11] Mohammad Hammoudeh, Robert Newman, "Adaptive routing in wireless sensor networks: QoSoptimisation for enhanced application performance", Information Fusion 22, Elsevier, Volume 22, PP. 3-15 March 2015.

[12] Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume 2013, pages 7

[13] Huang Lu, Jie Li, and Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Volume. 25, No. 3, PP. 750 – 761, March 2014

[14] Jun Zhao, Osman Ya ˘gan, Virgil Gligor, "Secure k-Connectivity in Wireless Sensor Networks under an On/Off Channel Model", IEEE International Symposium on Information Theory Proceedings (ISIT), PP. 2790 – 2794, 2013,

[15] Sankardas Roy, Mauro Conti, SanjeevSetia, and SushilJajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE Transactions on Information Forensics and Security, Volume. 9, No. 4, APRIL 2014

[16] Jun Zhao, Osman Ya–gan, Virgil Gligor, "Connectivity in Secure Wireless Sensor Networks under Transmission Constraints", Annual Allenton Conference on Communication, Control, and Computing (Allenton,), PP. 1294 – 1301, September 30- October 3, 2014, Monticello, IL

[17] Nabil Ali Alrajeh, Shafiullah Khan, Jaime Lloret, and Jonathan Loo, "Secure Routing Protocol Using Cross-Layer Design and Energy Harvesting in Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume, 11 pages, 2013.

[18] Huang Lu, Jie Li, and Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Volume 25, No. 3, MARCH 2014

[19] BASANT KUAMR VERMA, Dr. BINOD KUMAR, "A SURVEY ON WSN ROUTING AND ROUTING ATTACKS",INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER SCIENCE AND MANAGEMENT Vol. 1(2), July 2014

[20] Basant Kuamr Verma, Dr. Binod Kumar, "A Secure AdHoc Wireless Clustering Scheme for Improving Security", International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 3,March 2015

[21] BASANT KUAMR VERMA, Dr. BINOD KUMAR, "An Efficient Weighted Clustering Network For AdHoc Network", International Journal of Research in Computer Engineering and Electronics. Page 1, ISSN 2319-376X, VOl : 3 ISSUE : 5 (Sept-Oct'14)

[22] HarmanjitKaur, "Survey on Routing Protocols of Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, April 2015

[23] S.R. BoselinPrabhu, S. Sophia, "A Survey of Adaptive Distributed Clustering Algorithms for Wireless Sensor Networks", International Journal of Computer Science & Engineering Survey (IJCSES),Volume 2, No.4, November, 2011

[24] Prashant Kumar Maurya, Gaurav Sharma and MahendraSrivastava, "An Overview of AODV Routing Protocol", International Journal of Modern Engineering Research (IJMER), PP. 728-732, Volume 2, May-June, 2012

[25] RajuDutta, Shishir Gupta, Mukul K. Das, "Power Consumption and Maximizing Network Lifetime during Communication of Sensor Node in WSN", 2nd International Conference on Computer, Communication, Control and Information Technology (C3IT-2012), Volume 4, PP. 158-162, February 25 - 26, 2012.

[26] Sanjay K. Dhurandher, Isaac Woungang, RaveenaMathur and PrashantKhurana, "GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs", 27th International Conference on Advanced Information Networking and Applications Workshops, 2013

[27] Athira V Panicker, Jisha G, "Network Layer Attacks and Protection in MANET: A Survey", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 5, No. 3 PP. 3437-3443, 2014

[28] Yudhvir Singh, and DheerDhwaj Barak "Wormhole Attack Avoidance Technique in Mobile Ad-hoc Networks", 3rd International Conference on Advanced Computing and Communication

Technologies (ACCT), PP. 283 – 287, 6-7 April 2013, Rohtak

[29] Mohit Jain and HimanshuKandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks", International Conference on Advances in Computing, Control, & Telecommunication Technologies (ACT '09), PP. 555 – 558, 28-29 Dec. 2009, Trivandrum, Kerala

[30] Zubair Ahmed Khan, M. Hasan Islam, "Wormhole Attack: A new detection technique", 2012 International Conference on Emerging Technologies (ICET), PP. 1 – 6, Oct. 8-9, 2012, Islamabad

[31] VirenMahajan, MaitreyaNatu, and AdarshpalSethi, "Analysis of Wormhole Intrusion Attacks in MANETs", 2008 IEEE Military Communications Conference (MILCOM), PP. 1-7, 16-19 Nov. 2008, San Diego, CA

[32] Vikas Kumar Upadhyay, Rajesh Shukla, "An Assessment of Worm Hole attack over Mobile Ad-Hoc Network as serious threats", International Journal of Advanced Networking and Applications, Volume 5. PP. 1858-1866, 2013

[33] B.Revathi, D.Geetha, "A Survey of Cooperative Black and Gray hole Attack in MANET", International Journal of Computer Science and Management Research, Volume 1 September 2012

[34] Stephen Specht and Ruby Lee, "Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures", Technical Report CE-L2003-03, May 16, 2003.

Basant Kumar Verma obtained his Master degree from Department of Computer Science, Guru Ghasidas University, Bilaspur, Chhattisgarh, India in 2003. He is currently a Ph. D. student under the supervision of Dr. Binod Kumar. His research is centered on development of cluster-based intrusion detection system.