IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ESAODV: IMPLEMENTATION AND DESIGN OF SECURE AND EFFICIENT AODV FOR WSN

Mr. Ojashvi Shivwanshi*, Mr. Rahul Patel, Miss Preetika Saxena
CSE-AITR Indore, RGTU Bhopal
Indore Bypass Road, Mangiliya Square, Indore, M.P., India

DOI: 10.5281/zenodo.47043

ABSTRACT

A number of different network technologies are now in these days developed using the ad hoc configuration of networks. Among the wireless sensor network is one of most frequently used network technology for application developments. On the other hand the network devices are suffers from the various security and performance issues due to their ad hoc configurations. Therefore the solution for performance improvement and security concerns are required to investigate. In this presented work both the issues are included and a solution for providing efficiency and security is proposed. The proposed solution first performs the clustering in network. This approach keeps in track the performance of network nodes. To perform the clustering of mobile sensor network the weighted clustering approach is implemented. Additionally a malicious behaviour node tracking method is developed using the acknowledgment processing. During this communication the cryptographic manner of communication is used for providing full proof security. Thus the traditional AES algorithm is implemented for data cryptography and for security key exchange the DH algorithm is consumed. The implementation of the proposed routing technique is performed by manipulating the existing routing protocol namely AODV routing protocol. Additionally the simulation of the developed routing technique is demonstrated using the NS2 simulation environment. The experiments are evaluated with respect to the traditional AODV routing protocol under the attack conditions. Further for comparing the performance of both the networks the routing overhead, end to end delay, energy consumption, packet delivery ratio, and throughput is evaluated as the key performance factors. According to the experimentation results the proposed security technique successfully able to distinguish the attacker nodes and improve the performance even when the attacker is present in network.

KEYWORDS: Performance Improvement, Security, Black Hole, Gray Hole, Weighted Clustering Algorithm.

INTRODUCTION

A wireless sensor network is a distributed real-time system [1]. The network and their devices is changing self-according to the need of applications. Therefore different network configurations have changed dramatically. Most of the distributed systems follow the wired configurations of network. But the maintenance and installation of such kind of networks are cost effective. Therefore the wireless networks are becomes popular for providing network services in low installation and maintenance cost. The presented work is focused on the mobile wireless sensor networks where the power sources are limited, not works on real-time, and also having fixed set of resources. The wireless systems can be classified in two categories statically and ad-hoc. In ad hoc wireless systems are mobile and changing topology is property of network. Due to limited resources and frequent dynamicity it is expected the network is operating in efficient manner, to reduce the resources consumption.

On the other hand the ad hoc nature of network, frequently changing topology results two different and critical issues i.e. the performance losses of the network and the security concern related to network. During both the conditions the network performance is significantly affected. Therefore the proposed study is motivated to study about both the network issues. Therefore the proposed study is focused to improve the network performance improvement and finding the solution for reliable and secure technique for wireless sensor networks.

Wireless sensor network is collection of communicating nodes connected with wireless links to provide the information about the surroundings of the sensors. The sensor nodes or devices are developed with the limited amount of energy sources, computational units and the memory units. Therefore the efficiency is expected form the sensor network devices during their operations. Additionally for managing the mobility the network follows the concepts of ad hoc communication networks. Therefore the environment is always suspected for malicious attackers. Most of the attackers are utilizes the information of network routing protocols and using the routing information the attacker node performing their malicious work. In this presented work the Black Hole and Gray Hole attacks are considered for solution development.

The Black Hole is a serious kind of attack that advertises self as the shortest route among source and destination. Additionally when the source node discovers the route, for the destination node than the attacker replay to source immediately, due to this the source router is initiating the transmission through the malicious link. At the same time the malicious attacker just drop all the data transmitted to the Black Hole node. On the other hand during the deployment of Gray Hole attack the network router selectively drop the communicated packets. Therefore the security techniques are not recognizing the attack. Additionally that continuously degrades the performance of network. Thus both the attacks are serious issue in wireless sensor network.

Thus the proposed study involves the security investigation of wireless sensor network and their solution findings. The proposed solution involves the weighted clustering scheme for improving the performance of network and the cryptographic identity management provides the security during the communication. In this section the key working domain of the proposed work is described and in the next section the attack deployment and their analysis is reported.

ATTACK MODELS

This section involves the discussion about the attacks and their characteristics for the ad hoc networks specifically Black Hole and Gray Hole attack.

A. Black Hole attack

In Black Hole attack, using routing protocol to an attacker advertises itself as the shortest path to the target device. An attacker watches the routes request in a flooding based routing protocol. When the attacker receives an appeal for a route to the target node, it forms a respond involving of really short route. If the mischievous respond reaches the initiating node before the reply from the genuine node, a fake route gets created. Once the malicious device joins the network itself among the communicating nodes, it is bright to do anything with the packets passing through them. It can crash the packets between them to perform a denial-of-service attack, or on the other hand use its position over the route is the first step of man-in-the-middle attack.

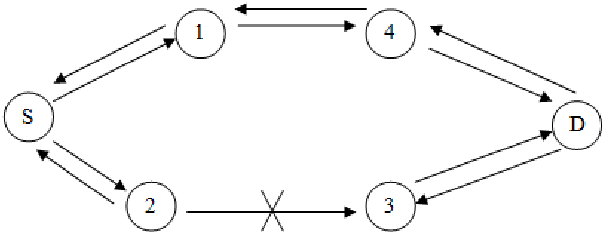

Figure 1 Black Hole Attacks

The Black Hole attack is a well-known security issue in WSN and MANET. The intruders develop the loophole to deploy their malicious activities because the route detection process is necessary and predictable. Many researchers have conducted different detection techniques to propose different types of detection schemes.

For example, in Figure 1, source node S wants to send data packets to destination node D and initiates the route detection process. Suppose that device 2 is a malicious device and it claims that it has a route to the destination whenever it receives route request packets, and straight away sends the reaction to node S. If the reply from the malicious node 2 influences firstly to node S, then node S considers that route detection is finished, than S ignores all other replies and starts to send data packets to node 2. As an outcome, all packets through the malicious node is consumed or lost.

B. Gray Hole Attack

Gray Hole attack is a variation of the Black Hole attack in which the malicious node may behave as an honest node first during the route discovery process and then may change its state to malicious and vice versa. This malicious node may then drop all or some of the data packets. The Gray Hole attack is difficult to detect due to congestion, overload and also due to malicious nature and ability of changing states. Gray Hole attacks are an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so and behaves like malicious node. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the some or all packets to launch a (DoS) denial of service attack. If neighbouring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehaviour. Gray Hole is a node that will act as a normal node that is actually an attacker node behaving like a Black Hole attack. So it is not easy to find the Gray Hole attack, since it behaves as a normal node. It is difficult to find out such kind of attack due to this type of behavior in the network. A routing table is maintained by every node that stores the information of the next node, which is a route towards the destination. The another name for Gray Hole attack is node misbehaving attack.

Types of Gray Hole Attack

In the Gray Hole attack nasty or malicious node is acting as normal node and drops the message or packets which is passing through them, hence hiding the important information to forward to the next node or destiny node.

- **Single Nasty Nodes:** In the Single Nasty Node, Selective Forwarding attack, is acting as nasty node and dropping selective packets.
- **Two Consecutive Nasty Nodes:** Two consecutive Nodes acting as nasty nodes, dropping packets and forwarding selective packets only.
- **Non-Consecutive Nasty Node:** Nodes are the non-consecutive nodes and they are acting as nasty node of the attacker, which forward or drops the selective packets on Network.
- **Surrounding Nasty Node:** In Surrounding Nasty Nodes attack, sometimes attackers affect the forwarding of the Selective packets in influence of the surrounding Nodes.

Gray Hole can be further divided according to dropping of Packets

1. Drops Packets of some specified node.
2. Drops Packets of some specified types.

PROPOSED TECHNIQUE

In order to obtain the solution for performance improvement of the wireless sensor network and for recovering the network from the Black Hole and Gray Hole attack. This section provides the detailed discussion about the proposed solution methodology. The proposed solution incorporates the three major modules for finding the optimum solution for both issues i.e. performance and security against Black Hole and Gray Hole attack. The three step solution involves the clustering of network, secure route identification and finally the cryptographic key exchange process.

A. Cluster Formation

According to the collected literature the network clustering is helps to improve the performance for the mobile wireless sensor networks. Therefore a number of different kinds of clustering approaches are available. Among them the weighted clustering algorithm provides conditional clustering based on the node quality evaluation and their parametric variations. Therefore it is required to select effective parameters to develop better resource preservation methodology. For the proposed solution the utilized parameters are defined as follows.

Connectivity:

In the context of network, the nodes are said to be connected, if the nodes are in radio range of neighbour nodes. Thus Maximum numbers of nodes are termed here as the connectivity of node. In other words the degree of nodes is known as the connectivity of the node. This parameter is selected because the higher connective node can serve for all the connected nodes. During the further discussion this parameter is given using C. Thus number of one hop nodes is considered for approximating the node degree or connectivity. For example a node labeled A has the connectivity value of 4 as demonstrated in the diagram 2. And similarly the node B has a degree of 3 for the demonstration.

Remain Energy:

The network devices in mobile WSN are created with limited energy. Additionally, if a node loses their energy frequently, then the node is not functioning as required. Thus it is required to make a cluster head with the higher energy or energy efficient node. Basically for each node event a significant amount of energy required. Thus remain energy is an essential parameter for clustering, that will be computed using the below given formula.

$$E = initial\ energy - lost\ energy$$

If the node energy is regulated according to the need thus the performance of network can be improvable in terms of energy consumption.

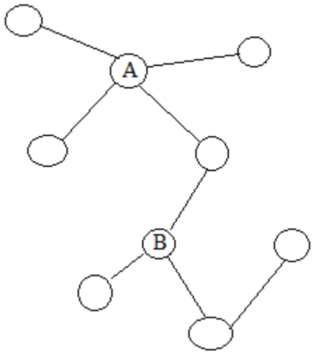

Figure 2 Connectivity

Mobility:

Another property of node in ad hoc network is mobility. Nodes are frequently moving from one place to other in this network randomly. The low mobile nodes are able to form more stable clusters. Because these nodes are connected with a long time, as compared to frequent mobile nodes, thus node mobility can be computed using the following formula.

$$M = \frac{1}{T}\sum_{i=1}^{T}\sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2}$$

Buffer length:

In network and socket programming the nodes are first accept the data using the buffer and for collecting information from the network that again utilizes the buffer. If the allocated buffer size of the node is consumed by the node that means a node in a high processing load or it suffers from the congestion problems thus the node which having less filled buffer can serve better as compared to filled buffer node.

Weight estimation

The estimated all the parameters are defined in different scales therefore the normalization process is required for combining these parameters. Therefore a weight is required to compute by which all the parameters are scaled on a similar scale. To compute weights also help to find the optimum node in network, thus a list of efficient nodes are created using the calculated weights.

$$W = w_1 * c + w_2 * E + w_3 * M + w_4 * B$$

In this weight calculation is performed by scaling the node performance parameters into a similar scale therefore $w_1, w_2, \ldots$ are providing the factors on with the nodes parameters are scaled. For constructing these factors the sum of these factors is required to be 1 and the distribution of these weights are between 0-1. After computing the weights for the all nodes the nodes are broadcast the weight information to their neighbour. The neighbours compare the weights to self-weight and other node’s weights. The higher weighted node is selected as the cluster head for the specified time interval.

B. Detection of secure route

After electing the efficient cluster heads, it is required to develop solution for Black Hole and Gray Hole attacker nodes. Therefore the initial working of the network is performed as the normal AODV. The AODV based route discovery is implemented to find out the best path to send data to all destination nodes. Therefore as AODV perform the RREQ request is flooded to the destination node and destination replay using RREP message. On the basis of this process the optimum path is selected. During this information exchange some additional information with the data packets are included such as packets IDs and time of receiving. The received packet at the destination now sends the acknowledgement to the source node using their neighbour nodes. If the data given to the destination node is original then the packet ID is matched with the previous packet id. Otherwise it may different from transmitted packet id. If sender node not receive confirmation packet till 5 sent packets in a predefined time than, now CH check every info packet that node. And towards destination next hop mark as malicious node and remove from the path. Therefore the security check is implemented on traditional process of route discovery and successfully able to distinguish the malicious node or attacker node in network.

C. Cryptographic data exchange

Each node in network communicates the sensitive data during the entire process of communication. Additionally the network also carries the information about the malicious attacker. Therefore the discloser of information can affect the discovery of malicious node. Thus for improving the security during the communicated data the cryptographic technique is used. In this purpose the traditional AES algorithm is used encrypt the data and other information in network. Additionally for key exchange DH key exchange mechanism is used for preserving the key.

D. Proposed algorithm

The section describes the summarized steps of the proposed secure and efficient routing protocol. The key steps of the entire process are given as:

1. Each node estimate connectivity C, remain energy E, mobility M and remain buffer length B.
2. Compute the weight of self W
3. Broadcast the node weights to their one hop neighbour nodes
4. Nodes compare the weight self and others and declare the highly weighted node as cluster head
5. A source node initiate the route request through the cluster head
6. In replay receiver node add packet id received and the time of receiving in cryptographic manner using AES algorithm
7. Exchange the key using DH algorithm
8. Destination wait for acknowledgement
9. If acknowledgment not received
10. Node is labelled as malicious or lost
11. Else
12. Prepare the secure connection
13. End if

NETWORK SIMULATION

The section provides the understanding about the implementation of the proposed security technique using the network simulation tool. Thus the required configuration and settings are reported in this section.

A. Simulation Setup

In this section provides the desired network configuration for simulation of clustering scheme’s implementation using AODV routing protocol.

Table 1 Network Setup

Simulation properties	Values
Antenna model	Omni Antenna
Dimension	750 X 550
Radio-propagation	Two Ray Ground

Channel Type	Wireless Channel
No of Mobile Nodes	20, 50, 100
Routing protocol	AODV
Time of simulation	30.0 Sec.

B. Simulation scenario

In order to simulate the effects of the network suitable network scenarios are required. This section provides the simulation scenarios on which the proposed and traditional algorithms are used for experimentation. The experimentations are used for network performance evaluation and comparative study for ensuring the security of the proposed technique.

1. The implementation of the traditional AODV routing based network: in this phase the traditional AODV routing protocol is used for configuring the network. After network configuration the attacker node is deployed on network. The network generated trace file is further used for performance evaluation of network. The required network scenario of the traditional AODV based routing is given using figure 3.

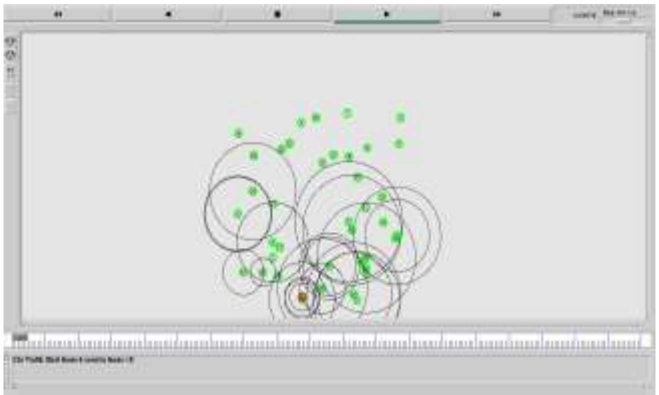

Figure 3 AODV under Attack

In this diagram the green color nodes shows the normal functioning nodes, additionally for demonstrating the malicious node in network the red color node is used. This provides the worst condition of the network and the parameters affected by the normal network during the attack conditions.

2. Implementation of the proposed AODV routing based security: in this phase similar kind of network is configured as demonstrated in the traditional AODV based network. The scenario demonstration of network as given in figure 4 only the difference among both the networks is that the given network is configured on the basis of the proposed cluster based secure routing technique. The modified AODV routing protocol is used with the attacker node (denoted using the red color node) is deployed on network. After that the network performance is evaluated using the network generated trace file. In this network the green nodes shows the normal functional nodes.

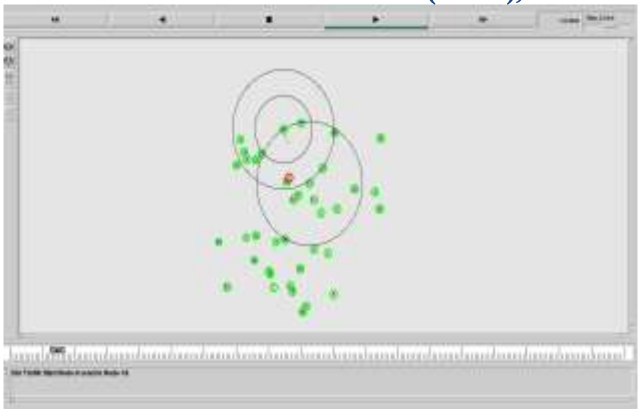

Figure 4 Proposed Technique under Black Hole Attack

RESULTS ANALYSIS

The chapter introduces about the analysis of performance of both the systems, additionally that describes the evaluated parameters for demonstrating the effect of the network performance during the descried simulation scenarios.

A. End to end delay

End to end day on network refers to the time taken, for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

$$E2E\ delay = receiving\ time - sending\ time$$

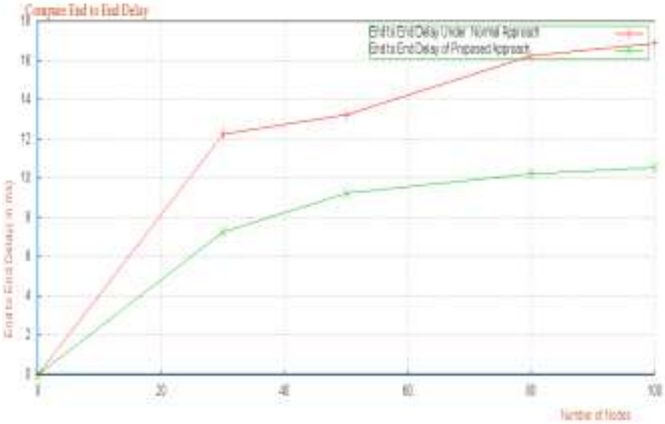

Figure 5 End to End Delay

The end to end delays of both the network scenarios are demonstrated using the figure 5. In this diagram the performance of normal AODV configured network is given by the red line and the performance of the proposed technique is given by the green line. In order to represent the performance of network the X axis contains the number of nodes in the network and the Y axis shows the corresponding time required for data transmission. According to the obtained results the proposed technique produces less amount of delay for data transmission as compared to normal AODV routing during the attack conditions. Therefore during the attacks the end to end delay of network is increases but the proposed routing technique keep in track the performance of network.

B. Remain energy

The amount of energy deduced from initial energy of nodes during the active communication sessions of network is known as energy consumption. The energy consumption is responsible to provide the efficient network life time. The energy consumption of both the configured network is demonstrated using the figure 6. In this diagram the X axis shows the number of nodes in network and the Y axis contains the amount of energy consumed during the simulation of network under attack conditions. For representing the performance of the routing protocols the red line denotes the performance of traditional AODV routing and the Green line shows the energy consumption of the proposed routing technique. According to the experimental results with the increasing number of nodes the energy consumption of the network remains consistent but the consumption of energy is increases in case of traditional AODV routing protocol. Thus the proposed technique not only effective for securing the network from assumed attacks (i.e. Black Hole and Gray Hole attack) that provides long network life time also.

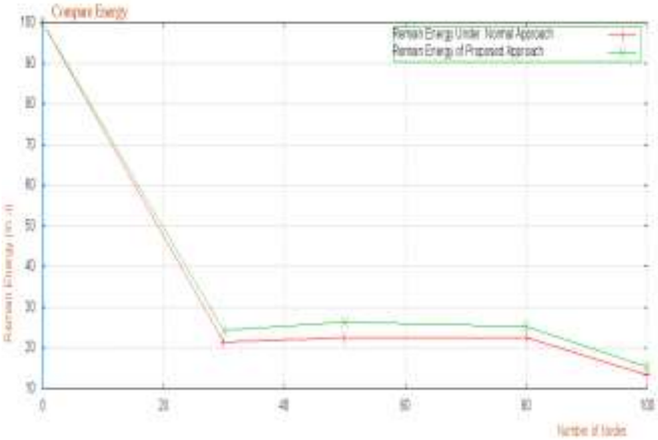

Figure 6 Remain Energy

C. Packet delivery ratio

The performance parameter Packet delivery ratio sometimes termed as the PDR ratio provides information about the performance of any routing protocols by the successfully delivered packets to the destination, where PDR can be estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

The packet delivery ratio of the traditional AODV routing technique and the proposed secure cluster based routing technique is demonstrated using the figure 7.

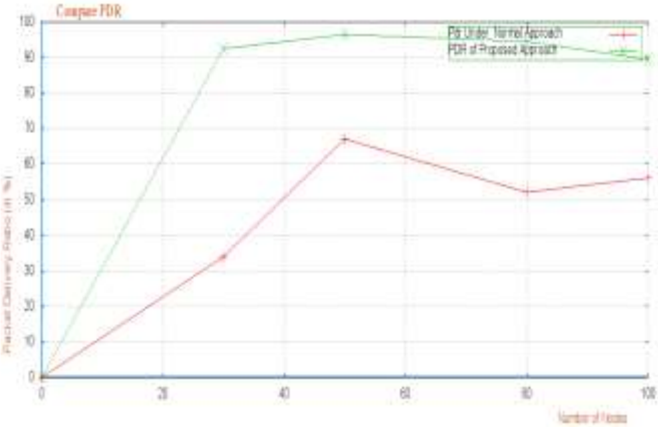

Figure 5.3 Packet Delivery Ratio

In this diagram the performance of the AODV routing protocol is defined using red line and the performance of proposed technique is demonstrated using the green line. For representing the performance of network the X axis contains the number of nodes in network additionally the Y axis shows the amount of packet delivered in network in terms of percentage. According to the experimental results the proposed algorithm is able to transmit a significant amount of data as compared to the traditional AODV routing technique therefore the proposed technique much efficient as compared to the traditional technique. In addition of that the losses occurred by the malicious attackers are also prevented using the proposed technique. Thus proposed technique is demonstrating the security concern of the network and also responsible for improving the performance of network.

D. Routing overhead

The amount of additional packets are injected in the network during the network activities is termed here as the routing overhead. The routing overhead of the proposed secure cluster based routing technique and the traditional AODV routing technique is given using figure 8. For demonstration of the performance of both the routing protocols the network is configured with the different numbers of node and the experimental observations are collected. The X axis of the experimental observation contains the amount of nodes participating in the network and the Y axis shows the amount of additional packets injected in network. The given performance of networks is measured in terms of percentage. Additionally for demonstration of performance the green line shows the performance of the proposed technique and the red line shows the performance of AODV routing. According to the observations the AODV produces more routing overhead as compared to the proposed technique. Thus the proposed secure cluster based routing is secure as well as efficient in terms of route establishment.

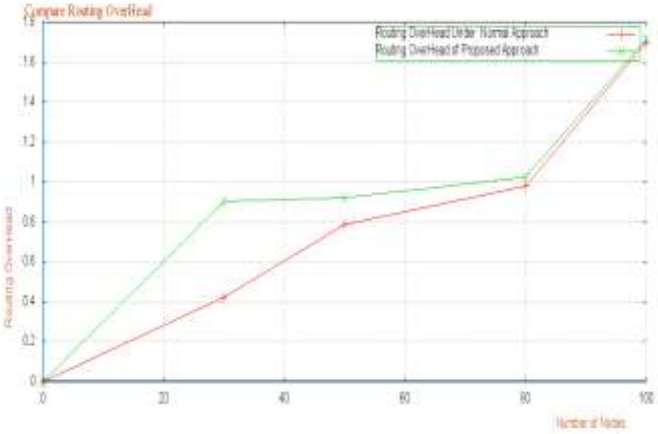

Figure 8 Routing Overhead

E. Throughput

Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. The throughput of both the network traditional AODV, and proposed secure routing technique is compared using the figure 9. The given diagram contains the different number of nodes in X axis and their respective performance in Y axis. In addition of the performance of the proposed technique is given using the green color line and the performance of traditional AODV routing is given using red line. According to the experimental evaluation the throughput of the traditional network under the attack conditions remains very low because very fewer packets are received at the destination thus the bandwidth consumption of the network is also becomes very low. On the other hand the proposed technique able to deliver the data even the attacker node exist in the network thus the proposed technique successfully reduce the impact of the attacker in network. Additionally provides efficient bandwidth consumption in network.

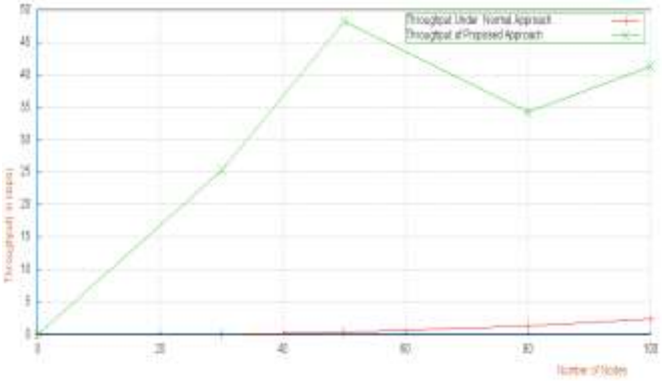

Figure 9 Throughput

CONCLUSIONS

The proposed study is dedicated to investigate about the security concern and the performance issues of the wireless sensor network and design of an enhanced routing protocol by which both the issues are resolved. This chapter provides the summary of the entire work performed for achieving both the goals. Thus the experimental and observational facts are included additionally the possible future extension is also suggested.

A. Conclusion

The wireless sensor network is one of the most popular network technologies therefore that are used in various different kinds of application development. According to their applications the surroundings of network and device configurations are affected. In this presented work the ad hoc wireless sensor network is considered for problem formulation and solution development. In such kind of networks the mobility based losses and the securities are the basic and classical issues to remain fixing. Thus the prospective of archiving both the goals the proposed solution is formulated.

The proposed security and performance improvement technique involve three main contributions in the network solution.

1. For performance improvement of the wireless sensor network the clustering of the network is performed using the weighted clustering algorithm which includes the mobility M, connectivity C, remaining energy E and buffer length for estimating the efficient and reliable cluster head
2. A secure route discovery using the cryptographic data exchange using AES algorithm
3. A secure key exchange technique using the DH algorithm

All the given contributions are included in network using the AODV routing protocol. Therefore the route discovery phase of the AODV routing is improved. Finally the implementation of the proposed secure and efficient routing protocol is performed using the NS2 (network simulator version 2.34). Additionally using the network traces the performance is measured and compared with the traditional AODV routing protocol. The comparative performance of network demonstrates the effectiveness of the proposed routing protocol additionally that is also provide the security during the data communication. The obtained performance of both the implemented routing protocols is summarized using the table 2.

Table 2 performance summary

S. No.	Parameters	Proposed routing	AODV routing
1	Throughput	High	Low
2	End to end delay	Low	High
3	Packet delivery ratio	High	Low
4	Routing overhead	Low	High
5	Energy consumption	Low	High

The proposed technique is found optimal for improving the performance of network and securing the network against the Black Hole and Gray Hole attacks. Thus the solution is adoptable for wireless sensor network and mobile ad hoc network both.

B. Future work

The proposed solution adoptable for network performance improvement and security for the Black Hole and Gray Hole attacks in ad hoc nature networks. In near future the proposed technique is enhanced more to incorporate more the attacks to secure the network.

REFERENCES

[1] M. Li, Z. Li, and A. V. Vasilakos, "A Survey on Topology Control in Wireless Sensor Networks: Taxonomy, Comparative Study, and Open Issues", Proceedings of the IEEE | vol. 101, no. 12, December 2013

[2] H. Lu, J. Li, and M. Guizani, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, vol.25, no. 3, March 2014

[3] C. Townsend, S. Arms, “Wireless Sensor Networks: Principles and Applications”, 10/2/2004 4:05:52 PM, WilsonChapter22.indd 439

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

[5] T. Arampatzis, J. Lygeros, and S. Manesis, “A Survey of Applications of Wireless Sensors and Wireless Sensor Networks”, Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005,0-7803-8936-0/05/$20.00 ©2005 IEEE

[6] L. J. G. Villalba, A. L. S. Orozco, A. T. Cabrera and C. J .B. Abbas, ”Routing Protocols in Wireless Sensor Networks”, Int.Journal of Sensors,vol.9,pp. 8399-8421

[7] K. Akkaya and M. Younis, "A Survey of Routing Protocols in Wireless Sensor Networks”, in the Elsevier Ad Hoc Network Journal, vol. 3/3 ,pp. 325-349, 2005

[8] A. Abbasi, M. Younis, “A Survey on Clustering Algorithms for Wireless Sensor Networks, ”in Elsevier Computer Networks Computer Communications, vol. 30, pp. 2826-2841, October 2007.

[9] Y. Zhao, J. Wu, F. Li, and S. Lu, “On Maximizing the Lifetime of Wireless Sensor Networks Using Virtual Backbone Scheduling”, Transection On Parallel and Distributed Processing, vol. 23, no 8, Month June Year 2012

[10] R. K. Bar, J. K. Mandal, and M. M. Singh, “QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack”, International Conference on Computational Intelligence: Modeling Techniques and Applications CIMTA) 2013

[11] D. N. Priyadharsini, L. D. MCA., “A Honey-Pot Server Based Black Hole Attack Detection in AODV Based MANETs”, International Journal of Computer Science and Mobile Computing, vol.3 Issue.10, October-2014, pp. 710-717

[12] R. Patel, M. Patel, “A Survey on Preventing DSR Protocol against Black Hole Attack for MANET”, International Research Journal of Engineering and Technology (IRJET), vol: 02 Issue: 09 | Dec-2015

[13] K. Bawa and S. B. Rana, “Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization”, International Journal of Current Engineering and Technology, 1 July 2015, vol.5, no.4 (Aug 2015)

[14] C. Joseph, P. C. Kishoreraja, R. Baskar and M. Reji, “Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios”, Indian Journal of Science and Technology, vol 8(29), DOI: 10.17485/ijst/2015/v8i29/84653, November 2015

[15] R. Rani, P. Dolly, D. Kumar, “Black Hole Prevention & Detection under Average Energy Consumption in WSN”, International Journal of Computer Science and Mobile Computing, vol.4 Issue.6, June- 2015, pp. 822-828

[16] S. Vhora, R. Patel, N. Patel, “Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET”, 978-1-4799-608S-9/1S/$31.00©2015 IEEE

[17] S. Dixit, K. K. Joshi and N. Joshi, “A Review: Black Hole & Gray Hole Attack in MANET”, International Journal of Future Generation Communication and Networking vol. 8, no. 4 (2015), pp. 287-294

[18] A. Rana, V. Rana , S. Gupta, “EMAODV: Technique to Prevent Collaborative Attacks in MANETs”, 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015

[19] P. K. Maurya, G. Sharma, V. Sahu, A. Roberts, and M. Srivastava, “An Overview of AODV Routing Protocol”, International Journal of Modern Engineering Research (IJMER), vol.2, Issue.3, May-June 2012 pp-728-732

[20] A. K. Mishra, and R. R. Singh, “Performance Analysis of Traffic Load and Mobility on AODV, DSR and DSDV Routing Protocols in MANET”, International Journal of Advance Research in Computer Science and Management Studies, vol 3, Issue 9, September 2015.