IJARCCE

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

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 5, May 2016*

# Detecting and Preventing Black hole and Grey Hole Attacks for Trust Management in Wireless Sensor Networks: A Survey

**Mitali Khandelwal[1], Sachin Upadhyay[2]**

PG Scholar, Computer Science Engineering, Alpine Institute of Technology, Ujjain, India [1]

Assistant Professor, Computer Science Engineering, Alpine Institute of Technology, Ujjain India [2]

**Abstract:** The wireless sensor network is one of the most popular network technologies for different applications. A number of applications such as weather monitoring and geo-location tracking are implemented using the WSN technology. Due to this these networks are utilized in critical situations. Therefore, the security in the communicated data is a primary aspect of the network as the performance of the network. Therefore, in this work the wireless sensor network security is investigated and a new secure routing technique is proposed for securing the data transmitted over the network. For providing the security a Trust and Opinion based approach is employed on network. This document provides the formal overview and the solution steps which are required to incorporate with the secure routing.

## I. INTRODUCTION

### 1.1 Wireless Sensor Networks

Wireless sensor networks as a part of MANET consists of a large number of tiny sensor nodes that continuously monitors environmental conditions. Sensor nodes perform various significant tasks as signal processing, computation, and network self-configuration to expand network coverage and strengthen its scalability.

The sensors all together provide global scenario of the environments that offer more information than those provided by independently operating sensors. They are also responsible for sensing environment and transmission information. WSNs are useful in various critical domains such as environment, industry, military, healthcare, security and many others. For an instance, in a military operation, a wireless sensor network monitors several activities [1].

WSN follows various topologies like star network, multi hop wireless mesh network etc. according to the requirements. For low cost infrastructure WSN uses low cost embedded devices, which are small in size and works on wide range of applications.

Therefore, they do not depend on any pre-existing infrastructure. WSNs have centralized approach in terms of network control. Data flows from sensor nodes towards a few aggregation points which further forward the data to base stations. Also base stations could broadcast query/control information to sensor nodes [2].

Wireless Sensor Network works in environment conditions especially where wired connections are not possible. Wireless sensor nodes consist of different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of physical and environmental conditions [3]

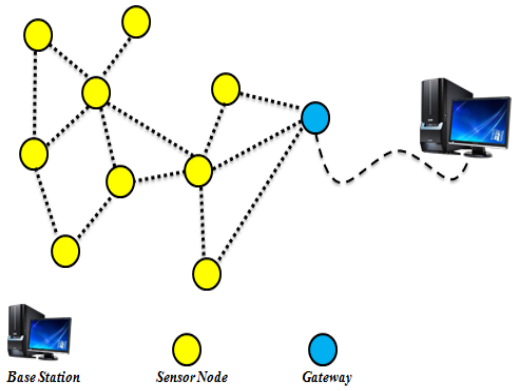


Figure 1 a typical View of WSN [3]

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Wireless sensor nodes contain array of sensors in case of multiple data collection. The sensor node can be put for continuous or selective sensing, location sensing, motion sensing and event detection etc. A base station links the sensor network to sense, process and disseminate information of targeted physical environments. Therefore, wireless sensor network plays a great role in order to send, receive and recover the data in networking.

### 1.2. Routing in WSN

Due to random infrastructure WSN routing has the responsibility to overcome from the situation of link failure, sensor node failure, battery destruction etc.

Therefore, the routing protocols can be implemented in various categories to work in different challenging conditions like Location based protocols, Data centric protocols, Hierarchical protocols, multipath based protocols, QOS based protocols [4]. All there protocols are further implemented in various ways shown below:

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 5, May 2016*

**1.2.1 Location Based Protocols**
To calculate the energy consumption, location information of sensor nodes are required by various routing protocols due to which we can calculate the distance between two particular nodes and then total energy consumption can be estimated[5]. To accomplish this task the following protocols are mentioned below.

**a. Geographic Adaptive Fidelity (Gaf)**
In any network when several nodes works with sensors to deliver or receive any message then there are three types of states found in sensor field i.e., sleeping, active and discovery. So when sleeping state comes then the sensor sensed it and turns off the radio waves to avoid unnecessary other sensors which are participating at the same time.

**b. Geographic and Energy Aware Routing (Gear)**
This routing protocol works on the basis of heuristic record of sensor nodes which is based on their location and energy consumption capacity. With the help of hardware like GPS unit it gathers the information about location and energy consumption. Then it fires query to find the appropriate path which saves energy.

**1.2.2 Data Centric Protocols**
This protocol has various appropriate data responders therefore the source sender sends its data to the sink independently to all other sensors. Then the intermediate sensors perform aggregation on the data which is originating from multiple source senders and then all aggregated data forwarded to the sink. It also saves energy due to less transmission requirements [5]. Some of these protocols are given below.

**a. Sensor Protocols for Information via Negotiation (Spin)**
This protocol is basically designed to overcome the problems like flooding, implosion, overlap etc. The sensor used in this protocol computes the energy requirement to compute send and receive data over the network. This protocol works on two main mechanisms i.e. negotiation and resource adaptation. So to overcome from redundant data supply and to avoid useless data, Negotiation works before sending any data packet.

**b. Rumour Routing**
In any network there is a long lived packet called agent, traverse through network. These agents inform entire network sensors about encounter and information gain during network traverse. It dies when crosses certain limit of number of hops Therefore when sensors and agents meats then they synchronise their list. Also sensors examine and update its list with agent in order to get shortest path.

**1.3 Security Issues of WSN**
There are various scenarios like military etc. where the confidential information needs to be maintaining with some privacy level. Therefore, there are various issues in WSN to maintain security, mention below-

**Data Confidentiality**
Confidentiality is an acceptance of authorized access to information communicated from a certified sender to a certified receiver. A sensor network must not reveal sensor readings to its neighbours. Highly sensitive data is sometimes routed through many nodes before reaching the final node. For secure communication, encryption is used. Data is encrypted with a secret key that only authorized users have [6]. Public sensor information should also be encrypted to some degree to protect against traffic analysis attacks.

**Data Integrity**
Provision of data confidentiality stops the outflow of information [7], but it is not helpful against adding of data in the original message by attacker. Integrity of data needs to be assured in sensor networks, which strengthens that the received data has not been tampered with and that new data has not been added to the original contents of the packet. Data integrity can be provided by Message Authentication Code (MAC).

**Data Authentication**
An adversary is not only limited to modify the data packet but it can change the complete packet stream by adding extra packets. So the receiver needs to confirm that the data used in any decision-making process comes from the authorized source [8]. Data authenticity is an assurance of the identities of communicating nodes. Nodes taking part in the communication must be capable of recognizing and rejecting the information from illegal nodes. Authentication is required for many administrative tasks.

**Data Freshness**
Data freshness ensures that the data communicated is recent and no previous messages have been replaced by an adversary. Data freshness is classified into two types based on the message ordering [9]; weak and strong freshness. Weak freshness provides only partial message ordering but gives no information related to the delay and latency of the message. Strong freshness on the other hand, gives complete request-response pair and allows the delay estimation. Sensor measurements require weak freshness, while strong freshness is needed for time synchronization within the network. For ensuring the freshness of a packet, a timestamp can be attached to it. Destination node can compare the timestamp with its own time clock and checks whether the packet is valid or not.

**Availability**
Availability is an insurance of the endowment to indulge expected services as they are designed earlier. It guarantees that the network services are feasible even in the subsistence of denial of service attacks. For making data available, security protocol should obsess less energy and storage, which can be targeted by the reuse of code and making sure that there is slight increase in communication due to the functioning of security protocols. Central point scheme should also be avoided as single point failure will be introduced due to this in a network that threatens the availability [8].

IJARCCE

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

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 5, May 2016*

**Self-Organization**
A typical WSN may have thousands of nodes fulfilling various operations, installed at different locations. Sensor networks are also ad hoc networks, having the same flexibility and extensibility. Sensor networks crave every sensor node to be independent and ductile enough to be self-organizing and self-healing according to different situations [8].

**Time Synchronization**
Most sensor network applications depend upon some form of time synchronization. In order to skimp power, an individual sensor's radio may be turned off for some time. Moreover, sensors may wish to calculate the end-to-end delay of a packet as it travels between two pair wise sensors [9].

**Flexibility**
Sensor networks will be used in vigorous arena scenarios where environmental circumstances, hazards and mission may change frequently. Changing mission goals may desire sensors to be eliminated from or injected to a settled sensor node. Moreover, two or more sensor networks may be merged into one, or a single network may be divided in two. Key establishment protocols must be ductile enough to render keying for all potential scenarios a sensor network may encounter [10].

## II. BACKGROUND

### 2.1 Black-hole Attack
While parsing data packet in any network every node has to communicate with data packet address frame to find reliable path in order to transfer data from source to destination. The intruders took the advantage and get the packet frame information and then carry out their malicious behaviour due to the necessity of route discovery process. The malicious node itself claims to deliver the message with shortest path. Then after gaining trust and data from data packet, it drops the packet although it has enough buffer storage. There may be two types of black hole attacks i.e. single and collaborative black hole attacks [11].

In single black hole attack there will be one malicious node on the path between source and destination. In collaborative black hole attack there may be no. of malicious nodes that supports each other to carry their malicious behaviour by dropping data packets and gaining trust without arousing suspicion[12].

Consider an example of black hole attack in which there is a network having some sensor nodes including source node, destination node and malicious node. Suppose node 1 is a source node and it wants to send a data packet to node 5 which is a destination node.

And there are two types of link between every node in the network, route request and route reply i.e. RREQ and RREP for connecting sensors nodes[13]. Shown in figure 2.

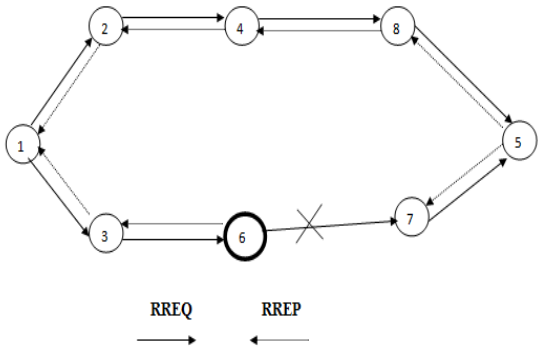

Figure 2 Black-hole Attack

Node 1 broadcast the data packet to its neighbour nodes i.e. node 2 and node 3 then this packet is further forwarded to node 4 and node 6, node 4 forwards it to get the destination and node 6 is malicious node therefore it claims to provide shortest path to the destination. Therefore, it sends reply as RREP link to node 3 and then this reply will further have forwarded to the source node, so source node selects the shortest path as malicious node suggested unknowingly. Now the source node will send the data packet reaches to node 6 via node 3. Now node 3 drops the packet instead of forwarding it to next nearest neighbour or destination [14].

### 2.2 Grey-hole Attack
In this attack node selectively drops the packet. In the network of nodes if any data packet lost occurs continuously then by traffic analysis it becomes easy to guess the malicious node. Therefore, grey-hole attackers drop the fraction of message selectively. There may be two conditions for selective forward attacks.

1) Malicious node can drop all UDP packets and forward TCP packets.
2) Dropping packets by following some probabilistic distribution.

Consider a scenario of grey-hole attack in which there is a network having some sensor nodes including source node, destination node and malicious node. Suppose node 1 is a source node and it wants to send a data packet to node 5 which is a destination node. And there are two types of link between every node in the network; route request and route reply i.e. RREQ and RREP for connecting sensors nodes[15]. Shown in figure 3

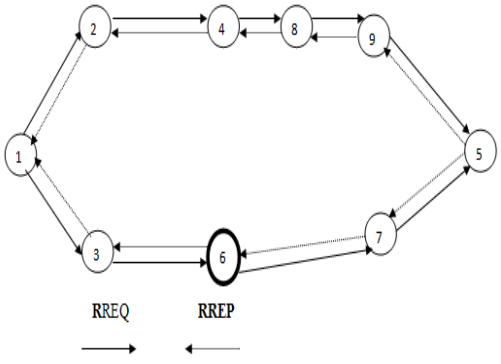

Figure 3 Grey-hole Attack

Node 1 broadcast the data packet to its neighbour nodes i.e. node 2 and node 3 then this packet is further forwarded to node 4 and node 6 Node 1 broadcast the data packet to its neighbour nodes i.e. node 2 and node 3 then this packet is further forwarded to node 4 and node 6, node4 forwards it to get the destination. Node 6 is malicious node so after getting the request from node 3, initially it behaves properly and forward the route request to the destination. Once the route is selected as shortest path via malicious node then it starts its malicious behaviour in various ways. It can drop the packet which is coming from specific source or which has to be reached to specific destination and then forward the entire remaining packet accurately from source to destination. Grey-hole attacker can show its misbehaviour as dropping data packet for certain fixed duration and after this duration again continue to forward the data packet from source to destination correctly. By possessing this kind of attack the attacker could be safe from arousing suspicion. Therefore the gray hole attach is more difficult to detect.

## III. LITERATURE SURVEY

**Determination Mechanism**

NishantSitapara et al. proposed a solution where black hole node is detected (assume) and tried to eliminate its effects. Solution tries to eliminate the black hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes begin the packets**.** Furthermore, author used UDP Connection to be able to count the packets at Sending nodes and receiving nodes**.**

If we will use the TCP connection between mobile nodes, the Sending node would be the end of the Connection, so ACK packets do not arrive at the sending node. This would be another solution for finding the black hole node. This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period. Author solution finds the path in the AODV level.

**Verify the Authenticity of Route the Route**

Deng et al. [17] proposed a solution for the black-hole attack problem in AODV routing protocol. They allowed the intermediate node to send a reply message if it had a fresh enough route to the destination. But the intermediate node could be a malicious node and could send route reply even if it had no fresh enough route to the destination to make a black hole attack. They proposed a solution that the source node would send another route request to the next hop of the intermediate node to verify the authenticity of the route from the intermediate node to the destination node. If the route exists, the intermediate node is trusted; otherwise, the reply message from the intermediate node is discarded. Sanjay Ramaswamy et al. **[18]** proposed a technique for identifying multiple black hole nodes inMANET. They are initially suggesting solution for cooperative black hole attack in ad-hoc network. Author in some extent modified AODV protocol by introducing data routing information table (DRI) and cross checking of routing table data where, each entry of the mobile node is maintained. They are depending on the trustworthy nodes to transmit the packets. Source sends The Route request (RREQ) to every node and it send packet to the node from where it gets the RREP. The intermediate node should send NHN and the DRI entry to the table. The source mobile node (SN) check own DRI table whether intermediate node (IN) node is trustworthy or not. In ad-hocnetwork, source node sending the supplementary request to next hop node (NHN) for IN (intermediate node). If SN uses IN to send the packet, then it is considered as trustworthy node otherwise not. Cross checking is done on the intermediate nodes and this is one-time procedure. The spending of cross checking is more and it can be making economical by letting mobile nodes sharing their trusted nodes record list with each other.

**Adaptive Path-based Technique**

Ning LIU et al. [19] proposed an adaptive approach to detect black and gray-hole attacks in ad hoc network based on a cross layer design network. In OSI network layer, a path-based technique to monitor the next hop's action. This method does not throw out extra control packets and saves the network system resources of the detecting mobile node. In network, The Media Access Control Layer a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. They decide to choose DSR protocol to test proposed algorithm and ns-2 as simulation tool.

**Issuing Security Certificate Approach**

Dr.E.Karthikeyan et al. [10] proposed solution that the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed technique is to be modified on DSR protocol and needs to be simulated and analysed for different performance parameters. This method is capable of detecting and removing black hole nodes in the MANET.

## IV. PROPOSED WORK

To detect the packet dropping attack for any sensor node we use opinion based technique in which will apply two conditions to decide whether the node is trustworthy or not. For which initially we took neighbour's reply for any destination including sample time. Then it stores the sequence number along with destination number and neighbour's IP. It also finds the packet delivery node ratio of neighbour's node. Initially the trust value of all the nodes is set as 0.0 i.e. same trust values for all the nodes.

For first condition, to trust any node's value it will compare the Packet delivery ratio of neighbour nodes and on the basis of packet delivery ratio it will increase or decrease the trust value of the node i.e. If the Packet delivery ratio is greater than certain threshold value then it will increase the trust value and if the packet delivery ratio is less than threshold than it will decrease the trust value. For second condition, along with trust value it also checks sequence no. i.e. if the current node receiving the reply

with same sequence number but the destination is not same than it may be malicious reply. Therefore, it will decrease the trust value of the node. Finally, when any transmission occurs then every node in the network applies these two checks. Therefore, if sender node found satisfactory trust value than it will forward the packet and if trust value is unsatisfactory than that node will be suspected as malicious node. Therefore, it will discard that node and search for another node to get secure transmission.

## V. CONCLUSION

There are various routing protocols in wireless sensor network which works to provide secure data packet transmission by selecting shortest path along with node failure recovery. Black hole attack and grey-hole attacks are more commonly found in any network which belongs to wireless sensor network. And it is the serious threat to wireless networks. We propose a solution to detect and avoid black hole and grey-hole attacks. This approach is basically designed to work against black hole and grey hole by observing packet delivery ratio and sequence number. Finally, after getting multiple replies from various nodes in network the node trustworthiness is decided on the basis of that replies to transmit the data packet.

## REFRENCES

[1]. PriyaMaidamwar and NekitaChavhan, "A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network", International Journal on Ad-Hoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012
[2]. Kia Xiang and ShyaamSundharRajamadam, "Attacks and Countermeasures in Sensor Networks: A Survey", pp 1-28, Springer, 2005.
[3]. Anjali Potnis, and C S Rajeshwari, "Wireless Sensor Network: Challenges, Issues and Research", Proceedings of 2015 International Conference on Future Computational Technologies (ICFCT'2015), pp. 224-228, March 29-30, Singapore, 2015.
[4]. Al-Shurman, M. Yoo, S. Park, "Black hole attack in Mobile Ad Hoc Networks" ACM Southeast Regional Conference, 2004, pp. 96-97.
[5]. Shiho Kumar Singh, M P Singh and D K Singh," Routing Protocol in Wireless Sensor Networks- A Survey " International Journal of Computer Science and Engineering Survey(IJCSES), vol.1, No.2.
[6]. Shio Kumar Singh, M P Singh, D K Singh, "A Survey on Network Security and Attack Defence Mechanism for Wireless Sensor Networks", International Journal of Computer Trends and Technology-, May to June Issue 2011
[7]. M. Yasir Malik, "An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations", Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management.
[8]. Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", IJCIT, vol. 2, issue 1, pp. 62-67, 2011
[9]. Pooja, Manisha, Dr.Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks", International Journal of P2P Network Trends and Technology, vol. 3, issue 1, pp. 7-13, 2013.
[10]. Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi, SarehBeheshti, "A Survey on Wireless Sensor Networks Security", SETIT 2007, 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 25-29, 2007 – TUNISIA
[11]. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey on balck hole attack in wireless mobile ad hoc network" (2011), Springer.
[12]. BounpadithKannhavong and Hidehisa Nakayama, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications October 2007, University of Washington
[13]. Fan-Hsun Tseng1, Li-Der Chou1and Han-Chieh Chao2, 3, 4" A survey of black hole attacks in wireless mobile ad-hoc networks".
[14]. E. A. Mary Anita and V. Vasudevan," Black Hole Attack Prevention in multicast routingProtocols for MANETs Using Certificate Chaining", IJCA, Vol.1, No.12, pp. 22–29,2010
[15]. Dharmendra Mishra, Deepak Sukheja, Sunil Patel, "A Review on Grey Hole Attack in Wireless Sensor Network."
[16]. Nishant Sitapara, Prof. Sandeep B. Vanjale,"Detection and Prevention of Black HoleAttack in Mobile Ad-Hoc Networks".
[17]. Hongmei Deng, Wei Li, and Dharma P.Agrawal "Routing Security in Wireless AdHoc Network" IEEE Communications Magzine, vol. 40, PP.70-75, 2002
[18]. Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and KendallNygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".
[19]. Wei Gong, Zhiyang You1, Danning Chen, Xibin Zhao, Ming Gu, Kwok-Yan Lam, "Trust Based Malicious Nodes Detection in MANET", 2009 IEEE
[20]. N. Bhalaji1, Dr. A. Shanmugam2," Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET". Journal of Advances in Information Technology, Vol. 2, No. 2, May 2011.