International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

AODV based Secure Algorithm for Detection and Prevention of Sink Hole Attack in WSN

Varpreet Kaur, Pratibha

Punjab Technical University, Sri Sukhmani Institute of Engineering and Technology, Derabassi, Punjab

Sri Sukhmani Institute of Engineering and Technology, Derabassi, Punjab, Punjab Technical University

Abstract: ***Wireless sensor network is a branch of networking that deals with sensing of information from deployed area. Sensor nodes collect the information by sensing the information and transmit using sink nodes. Sink nodes collects the information from sensor nodes and transmit this information to base station. In wireless sensor network various malicious nodes has been introduced to perform various types of attacks on the network to degrade or collect same information. The new attack that has been used for acquiring information by performing sinkhole attack. Sink hole attack is performed on sink node attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. Actual data doesn't receive at base station that loss the information of the network.***

Keywords: Wireless Sensor Network, AODV, DSDV, TORA, DSDV

1. Introduction

Wireless sensor network: A wireless sensor network is a wire and wireless system, which comprises of a few sensor nodes, sent in a specific field. A sensor node ought to have calculation, detecting and remote correspondence capacities. A wireless sensor network confines the radio recurrence channel, because of, that is to say, precarious connections, breaking point of physical assurance of every sensor node real of every nodes association, variety topology what's more risk about directing security is high by movement spite nodes. A sensor network has constrained figuring and correspondence assets. To defeat this obstruction, cooperation with encompassing nodes is required. As it were, data sharing between chains of importance is required as opposed to a various leveled approach.

A sensor network for the most part comprises of countless nodes for definite sensing and extendibility of sensing zones. Subsequently, aggressors can undoubtedly catch sensor nodes and the attacker can attack the sensor node itself and the sensor network through a changed attack on the sensor node. In this way, the security of a sensor network is imperative. Sensor networks are connected to different fields running from extraordinary application fields, for example, wild environment observing, mechanical machine estimation and military reason estimation to day by day application fields, for example, fire checks and pollution observing.

1.2 WSNs can be divided in two classes

1.2.1 Structured
1.2.2 Unstructured.

1.2.1 Structured WSN

In this, all sensor nodes are at fixed locations which requires lower network maintenance and management costs.

1.2.2 Unstructured WSN

It consists of dense sensor nodes which are placed into the field. An ad-hoc deployment is suitable over pre-planned deployment. Where network consists of hundreds to thousands nodes over a large area or when it is not accessible by humans to construct WSN, e.g. Polar Regions, deep sea, or disaster areas such as nuclear accident area or a war zone. Today's WSNs is being used for remote environmental monitoring and target tracking. This has been enabled by the availability of sensors that are smaller, cheaper, and intelligent.

1.3 Applications of Wireless Sensor Network

1.3.1 Process Management

The common application of WSN is area monitoring. In area monitoring, the WSN is deployed ahead an area where a number of phenomenon is to be monitored. The utilize of sensors detects enemy intrusion is mil; a civilian example is the geo-fencing of gas or oil pipelines. Area monitoring is most imperative part.

1.3.2 Health care monitoring

The medical application of two types: wearable and rooted. First device are used on the body surface of a human and also just at close proximity of the user. The implantable medical devices are those which are inserted within the human body. There are also many other application like body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can assemble whole information about an individual's health, fitness, and energy expenditure.

1.3.3Environmental/Earth sensing

In monitoring environment there is application, which deals with the extra challenges of harsh environments and reduced power supply.

1.3.4Air pollution monitoring
Wireless sensor networks have been deploying in several cities to supervise the amount of dangerous gases that is hazard to citizens. That is one of the advantages of the ad hoc wireless links rather than wired installations, which also make them mobiles more efficient that is used for testing readings in different areas.

1.3.5Forest fire detection
A network of Sensor Nodes can be installed in a forest to identify when and how fire has been started. The nodes can be prepared with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is vital for a successful action to the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is scattering.

1.3.6Landslide detection
A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and change in various parameters that may occur before or during a landslide. Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.

1.3.7Water quality monitoring
Water quality supervision involves the process Of determine water properties in dams, rivers, lakes & oceans, as well as underground water reserves. The utilization of many wireless distributed sensors that enables the formation of a more accurate map of the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, without the need of manual data recovery.

1.4 Attacks in Wireless Sensor Networks

There are various kinds of attack that can influence the entire system or can humiliate the performance of system. The attacks can be categorized into following types.

1.4.1 Denial of Service attack
This strike happens when the aggressor increment control of a vehicle's benefits or jams the channel of correspondence utilization by the Vehicular Network, so it makes twist to send separating information to its end of the line. It additionally expands the threat to the driver, on the off chance that it needs to rely on upon the application's data. For example, in the event that a nasty needs to make a colossal load up on the roadway, it can make a disaster and use the Dos strike to keep the forewarn from landing at to the approaching vehicles. Creator in [1] talked about an answer for Dos issue and saying that the current arrangements, for example, bouncing don't totally deal with the issue, the consumption of different radio handsets, working in disjoint recurrence groups, can be a feasible approach yet even this course of action will oblige adding new and more apparatus to the vehicles, and this will require more sponsors and more space in the vehicle. The inventors in [12], proposed an answer by trading between assorted channels or even correspondence progresses (e.g., DSRC, UTRA-TDD, or even Bluetooth for short ranges), in case they are open, when one of them (routinely DSRC) is chop down.

1.4.2 Message Suppression Attack
An assailant particularly dropping packets from the system, these bundles may hold discrimination of data for the recipient, the aggressor suppress these parcels and can utilize them again as a part of other time. The objective of such an assailant would be to keep enrollment and protection powers from looking into crashes including his vehicle and/or to withdraw from conveying crash reports to roadside access focus. Case in point, an aggressor may suffocate a blockage threatening, and use it in an alternate time, so vehicles won't get the cautioning and forced to hold up in the activity.

1.4.3Fabrication Attack
An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could declare that it is another person. These assaults incorporate create messages, warnings, declarations, personality [1].

1.4.4Alteration Attack
This assault happens when aggressors modify current information, it incorporates defer the transmission of the data, replay subsequent transmission, or changing the genuine section of the information transmitted [1]. For example, an aggressor can modify a message telling different vehicles that the present street is clear while the street is congested [2].

1.4.5Replay Attack
This assault happens when an aggressor repeat the transmission of a prior data to exploit the conditions of the message at time of sending [2].

1.4.6Black hole Attack
When some wicked user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node.

1.4.7Grey hole Attack
This attack occurs if some node falling 50% of the packets and rest 50% is sending by varying the message. In this way wrong information is transmit.

1.4.8Sybil Attack
In this attack, attacker generates multiple identities to replicate multiple nodes. Each node send messages with multiple identities, in this way other nodes realize that there are many nodes in the network at the same time. This attack is very hazardous because a one node can give its various locations at the same time and this creating security risk.

1.4.9Sink Hole Attack
In Sink Hole attack malicious node acts as a black hole to draw all the traffic in the sensor network. Attacker listens to requests for routes then reply to the target nodes. It inserts itself between the communicating nodes; it is able to do anything with the packets passing between them.

1.4.10 Cloning attack

A node replication attack involves an attacker inserting a new node into a network which has been clone from an existing node, such cloning is being a comparatively simple task with current sensor node hardware. This new node can act precisely like the old node or it can have some extra behavior.

2. Review of Literature

Vandana B. Salve,et.al[1] "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks" in this paper represent the Wireless sensor Networks consist of small nodes with sensing, computation and wireless communication wireless capability. This paper present an AODV based on protected routing algorithm based on mobile agent for detecting the malicious node in sinkhole attack. The algorithm detect sinkhole node by finding the difference of nodes sequence numbers using threshold value. It also shows performance estimation of AODV with the superior secure routing algorithm and existing secure routing algorithm through simulations, which confirmed the efficiency and exactness of the algorithm by taking into consideration performance metrics as Throughput, PDR and Packet loss. Simulation is carried out using simulator NS2.

Ahmad Salehi S. et.al.[2] "Detection of Sinkhole Attack in Wireless Sensor Networks" Generally wireless sensor networks rely of Manito- one communication approach for data gathering. This approach is exceptionally susceptible to sinkhole attack, where intruders attract surrounding nodes with unfaithful routing information, and subsequently presents selective forwarding or change the data that carry through it. A sinkhole attack cause an significant threat to sensor networks and it should be considered that the sensor nodes are mostly spread out in open areas and of weak computation and battery power. In order to observe the intruder in a sinkhole attack this paper suggests an algorithm which firstly finds a group of assumed nodes by analyze the uniformity of data. Then, the intruder is documented efficiently in the group by checking the network flow information.

A.Vijayalakshmi. et.al.[3] "Mobile Agent Middleware Security for Wireless Sensor Networks" Wireless Sensor Networks have gain much consideration in recent applications. However, they are very much subjected to the security threats. To provide security planning in sensor nodes, the energy required to carry out the operation may reduce the life time of the sensor nodes. In order to optimize the energy usage in sensor nodes, Middleware concept is introduced. The Middleware to provide security for the Wireless Sensor Networks is arranged in the Mobile agent with the capability of optimizing the power usage with the sensor nodes. An energy efficient Mobile agent based algorithm is simulated. It will be recognized that the Mobile agents provide the security measures to the Wireless sensor networks for the reduction of sinkhole and cloning attacks.

Van dana B. Salve,et.al.[4] "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks" Wireless sensor Networks consist of small nodes with sensing, computation and wireless communication wireless capabilities. This paper present an AODV based secure routing algorithm based on mobile agent in favor to detect the malicious node in sinkhole attack. The algorithm detect sinkhole node by finding the difference of nodes sequence numbers using threshold value. It also shows performance evaluation of AODV with the better secure routing algorithm and existing secure routing algorithm through simulations, which confirmed the usefulness and accuracy of the algorithm by considering performance metrics as Throughput, PDR and Packet loss. Simulation is carried out using simulator NS2.

Mohamed Guerroumi.et.al.[5] "Intrusion detection system against Sink Hole attack in wireless sensor networks with mobile sink" In this paper, we propose an Intrusion Detection System (IDS) against Sinkhole attack in wireless sensor networks with mobile sink. In the detection model, the network area is divided into a flat grid of cells, and we use the signature-based technique, which is represented by the detection rate of a cell, to make difference between real and fake sink nodes. The proposed IDS consider two types of sink mobility: periodic and random. In addition, as the cell leaders do not activate their IDS agent simultaneously, the additional energy consumption incurred by the IDS is low. Simulation results show the efficiency of the projected IDS in terms of detection rate, efficiency, and energy consumption.

Sheela D.et.al.[5] "A Non Cryptographic method of sink hole attack detection on wireless sensor network" A Wireless Sensor Network (WSN) consists of large number of low cost low power sensor nodes. The nature of wireless sensor networks makes them very attractive to attackers. One of the most popular and serious attacks in wireless sensor networks is sink hole attack and most existing protocols to defend against this attack used cryptographic methods with keys. In sink hole attack a sensor node will have a lot of false neighbors. Wireless Sensor Network has a dynamos topology, intermittent connectivity, and resource constrained device nodes. Researchers over the past years have encouraged the use of mobile agent to rise above these challenges. The proposed scheme is to preserve against sink hole attack using mobile agents. Mobile agent is a program segment which is self controlling.

3. Approaches Used

Dedicated short-range communications (DSRC)

Dedicated short-range communications are one-way short-range to medium-range wireless communication channels explicitly designed for automotive use and a related set of protocols and standards. DSRC/WAVE is the only wireless technology that can potentially meet the extremely short latency requirement for road safety messaging and control. The unique features of low latency secure the role of DSRC, As an essential communication technology, in future CALM networks that will make use of multi-radios on multi-bands.

However, the current DSRC solutions are not fully field proven.

Destination sequenced distance vector routing (DSDV)
DSDV is adapted from the conventional routing information protocol (RIP) to Ad- Hoc networks routing. It adds a new attribute, sequence number, to each route table entry of the predictable RIP. Using the newly added sequence number, the mobile nodes can make distinction stale route information from the new and thus prevent the formation of routing loops. Packet routing and routine table management in DSDV, each mobile node of an Ad-Hoc network maintains a table, which lists all available destinations, the metric and next hop each destination and a sequence number generated by the destination node. Using such routine table stored in each mobile node, the packets are transmitted between the nodes of an An-Hoc networks. Each node of the Ad-hoc network updates the routing table with advertisement occasionally or when significant new information is available to maintain the regularity of the routing table with the dynamically TORA (Temporally Ordered Routing)

The TORA attempts to achieve a high degree of scalability using a "FLAT", Non-Hierarchical routing algorithm. In its operation the algorithm attempts to hold back, to the greatest extent possible, the generation of comprehensive control message transmission. In order to achieve this, the TORA does not use a shortest path solution, an approach which is unusual for routing algorithms of this type. TORA builds and maintains a Directed Acyclic Graph (DAG) rooted at a destination. No two nodes may have the same height. Information may flow from nodes with higher heights to nodes with lower heights. Information can therefore be thought of as a fluid that may only flow downhill. By maintaining a set of totally ordered heights at all times, TORA achieves loop-free multipath routing, as information cannot 'flow uphill' and so cross back on itself. The key design concepts of TORA are localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain the routing information about adjacent (one hop) nodes. The protocol performs three basic functions:

Route creation
- Route maintenance
- Route erasure

AODV: The Ad hoc On-Demand Distance Vector (AODV) routing protocol provide unicast, broadcast, and multicast communication in ad hoc mobile networks. AODV initiates route discovery whenever a route is needed by a source node, or whenever a node wishes to join a multicast group. Routes are maintained as long as they are needed by the source node or as long as the multicast group exists, and the routes are always loop-free through the use of sequence numbers. AODV nodes maintain a route table in which next hop routing information for destination nodes is stored.

Dynamic Source Routing (DSR): Dynamic Source Routing is a Pure On-Demand routing protocol, where the route is calculated only when it is required. It is considered for use in multi-hop ad hoc networks of mobile nodes.DSR allows the network to be self organized and self configured without any central administration and network infrastructure. It uses no periodic routing messages like AODV, thus reduces bandwidth overhead and conserved battery power and also large routing updates. It only requests the effort from the MAC layer to identify link failure.DSR uses source routing where the whole route is carried as an overhead.

4. Conclusion

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Sensor nodes collect the information by sensing the information and transmit using sink nodes. Sink nodes collect the information from sensor nodes and broadcast this information to base station. The new attack that has been used for acquire information by performing sink hole attack. Sink hole attack is performed on sink node attacking node replace the actual sink node by advertising its availability and resumes all the data from the sensor node. Actual data doesn't receive at base station that loss the information of the network. The issue of sink hole attack detection scheme has to be implement that detect attacking node and routing algorithm for reliable communication over the network.

References

[1] Vandana B. Salve,"AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks" IEEE International Conference on Electrical, Computer and Communication Technologies,2015,pp- 1 – 7.
[2] Ahmad Salehi S. "Detection of Sinkhole Attack in Wireless Sensor Networks", IEEE International Conference on Space Science and Communication, 2013, pp. 361-365.
[3] A. Vijayalakshmi., "Mobile Agent Middleware Security for Wireless Sensor Networks" IEEE International Conference on Communication and Signal Processing, 2014, pp. 1669- 1673.
[4] Van dana B. Salve, "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks", IEEE International Conference on Electrical, Computer and Communication Technologies, 2015, pp. 1 – 7.
[5] Mohamed Guerroumi "Intrusion detection system against Sinkhole attack in wireless sensor networks with mobile sink" IEEE International Conference on Information Technology, 2015, pp. 307- 313.
[6] Sheela, D. "A non cryptographic method of sink hole attack detection in wireless sensor networks" IEEE International Conference on Information Technology, 2011, pp. 527 – 532.
[7] Guerroumi, M., "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink" IEEE International Conference on Information Technology - New Generations, 2015, pp. 307 – 313.

[8] Varshney, K.K. "Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network" IEEE International Conference on Information Communication and Embedded Systems, 2014, pp. 1 – 5.
[9] Yong-Sik Choi, "A study on sensor nodes attestation protocol in a Wireless Sensor Network", IEEE Conf. on Advanced Communication Technology (ICACT), 2010, pp. 1738-9445.
[10] Yuling Lei "The Research of Coverage Problems in Wireless Sensor Network", IEEE Conf. on Wireless Networks and Information Systems, 2009, pp 31 – 34.
[11] Mittal, R. "Wireless sensor networks for monitoring the environmental activities" IEEE Conf on Computational Intelligence and Computing Research (ICCIC), 2010, pp. 1 – 5.
[12] Marriwala, N. Rathee, P. "An approach to increase the wireless sensor network lifetime" IEEE Conf. on Information and Communication Technologies (WICT), 2012, 495 – 499.

Author Profile

Varpreet Kaur received the B.Tech. degree in Computer Science and Engineering from Sri Sukhmani Institute of Engineering & Technology, Dera Bassi in 2013 and pursuing M.Tech degree in Computer Science and Engineering from Sri Sukhmani Institute of Engineering & Technology, Dera Bassi.