INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON PREVENTIVE MEASURES FOR BLACKHOLE ATTACKS IN WIRELESS SENSOR NETWORK

PALLAVI A. DHANDE, PROF. GAURAV D. GULHANE, DR. H. R. DESHMUKH

CSE Department, DRGIT&R, Amravati, Maharashtra, India

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Wireless sensor networks are vulnerable against various types of external and internal attacks being limited by computation resources, smaller memory capacity, limited battery life, processing power & lack of tamper resistant packaging. The intruders utilize the loophole to carry out their malicious behaviours because the route discovery process is necessary and inevitable. The black hole attack is one of the well-known security threats in wireless sensor networks. Two types of black hole attacks single black hole attack and collaborative black hole attack are discuss. In this paper, we survey the existing solutions and discuss the state-of-the-art routing methods.

Keywords: Wireless Sensor Network, routing protocols collaborative, single black hole attack, black hole attack

Corresponding Author: MS. PALLAVI A. DHANDE

Access Online On:

www.ijpret.com

How to Cite This Article:

Pallavi A. Dhande, IJPRET, 2016; Volume 4(9): 1730-1743

PAPER-QR CODE

INTRODUCTION

Sensor networks [1][2][3] are highly distributed networks of small, lightweight wireless nodes, installed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or humidity. The applications of sensor networks are endless, limited only by the human imagination [1] [2] [3]. It is to be mentioned that all the attacks are mentioned thoroughly as well as the preventive measures mentioned in this paper is also not exhaustive. The rest of the paper is as follows: Section 2 gives design issue of WSN followed by section 3 in which various types of routing protocol in WSN are highlighted. In this paper an overview on various WSN attacks are mentioned with a special mention on black hole attack. Summery on the counterattacks and possible preventive measures are mentioned. In section 4 classification of black hole attack is described followed by in section 5 types of black hole attack and countermeasure on black holes are discussed. In section 6 open research challenge described and conclusion is stated in section 7. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes.

DESIGN ISSUES OF SENSOR NETWORKS

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing routing schemes. Due to the reduced computing, radio and battery resources of sensors, routing protocols in wireless sensor networks are expected to full fill the following requirements [4]. A wireless sensor network is a special network which has many constraint compared to a traditional computer network.

Autonomy: The assumption of a dedicated unit that controls the radio and routing resources does not stand in wireless sensor networks as it could be an easy point of attack. As there will not be any centralized entity to make the routing decision, the routing procedures are delivered to the network nodes.

Energy Efficiency: Routing protocols should persist network lifetime while maintaining a good grade of connectivity to allow the communication between the nodes. Under some circumstances, the sensors are unreachable. It is important to note that the battery replacement in the sensors is infeasible since most of the sensors are distributed. For instance, in wireless underground sensor network, some devices are deployed to make them able to sense the soil.

Scalability: Wireless sensor networks are composed of thousands of nodes so routing protocols should work with this amount of nodes.

Fault-tolerant: The Routing protocols should deals with this eventuality so when a current node fails, an alternative route should be discovered. Sensors may unpredictably stop operating due to environmental reasons or to the energy consumption.

Device Heterogeneity: Although most of the applications of wireless sensor network rely on homogenous nodes, the introduction of different kind of sensors could report significant benefits. Comparing with other networks, the scalability of the network, the energy drainage or bandwidth is very potential candidates to benefit from the heterogeneity of nodes. The use of nodes with different transceivers, processors, power units or sensing components may improve the characteristics of the network.

Mobility Adaptability: Routing protocols should provide appropriate support for these movements. The different applications of wireless sensor networks could demand nodes to deals with their mobility, the mobility of the sink or the mobility of the event to sense.

ROUTING PROTOCOLS

There are plenty and different routing protocols in WSN and kinds of investigations have been completed in recent decades. In this section, we introduce the famous and popular routing protocols in WSN. Before a mobile node wants to communicate with a destination node, it should broadcast its present status to the neighbours due to the current routing information is unfamiliar. As the information is acquired, the routing protocols is classified into proactive, reactive and hybrid routing.

1. Proactive (table-driven) Routing Protocol

The proactive routing is also called table-driven routing protocol. In other words, all of the nodes in the network have to evaluate their neighbourhoods as long as the network topology has changed. In this routing protocol, nodes time to time broadcast their routing information to the neighbors. Each node needs to maintain their routing table which not only records the adjacent nodes and reachable nodes but also the number of hops present in the network. Therefore, the drawback is that the

overhead increases as the network size increases, a large communication overhead within a larger network topology. The most common types of the proactive type are destination sequenced distance vector (DSDV) routing protocol and optimized link state routing (OLSR) protocol. But, the advantage is that network status can be immediately known if the malicious attacker joins.

2. Reactive (on-demand) Routing Protocol

The reactive routing is also named on-demand routing protocol. Unlike the table driven routing, the reactive routing is simply started when nodes desire to transmit data packets. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node is unreachable from the source node, the route discovery process will be performed immediately. The strong point is that the wasted bandwidth induced from the cyclically broadcast can be minimized. However, this might also be the serious wound when there are any malicious nodes in the network environmentIn the route discovery phase, the source node broadcasts the route request (RREQ) packet first and then all intermediate nodes receive the RREQ packets, but parts of them send the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. . The disadvantage is that passive routing method leads to some packet loss. Most common on-demand routing protocols which are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) protocol. Also, the route maintenance process is started when the network topology has changed or the connection has failed. The source node is observed by a route error (RRER) packet first. Then it uses the present routing information to choose a new routing path or restart the route discovery process for updating the information in routing table. Unlike AODV which only records the next hop information in the routing table, the mobile sensor nodes in DSR maintain their route cache from source to destination node. From above it is clear that, the routing path can be determined by source node because the routing information is recorded in the route cache at each node. The key idea of dynamic source routing (DSR) is based on source routing. The source routing is the each data packet contains the routing path from source to destination in their packet headers. However, the performance of DSR decreases with the mobility of network increases, lower is the packet delivery ratio higher will be the network mobility.

3. Hybrid Routing Protocol

The hybrid routing protocol combines the advantages of proactive routing and reactive routing to overcome the drawbacks of them. Most of hybrid routing protocols are designed as a hierarchical or layered network framework. The most commonly use hybrid routing protocols are zone routing protocol (ZRP) and temporally-ordered routing algorithm (TORA). In the beginning, proactive routing is working to completely gather the unfamiliar routing information, then by using the reactive routing to maintain the routing information when network topology changes.

CLASSIFICATION OF ATTACKS IN WSN

Attacks are classified into two categories active attacks and passive attacks. In passive attack acts as a passive attacker and doesn't harm the communication channel. In active attacks data alteration is occur. Passive attacks are most serious attack as the network is not aware with the attack. There are several active attacks as well as passive attacks found in each layer of ISO OSI model which can be shown in table[5].

Layer	Attacks	Security approaches
Physical Layer	Denial of Service Tampering	Priority Messages Tamper Proofing Hiding, Encryption [4].
Data Link Layer	Jamming Collision Traffic manipulation	Use Error Correcting Codes Use spread spectrum techniques
Network Layer	Sybil attack Wormhole attack Sinkhole Flooding	Authentication Authorization Identity certificates
Transport Layer	Resynchronization Packet injection attack	Packet Authentication

Application Layer	Aggregation based attacks Attacks on reliability		Cryptographic approach

LITERATURE REVIEW

	Author's Name	Evolution Approach
1.	M. Marina and S. Das	proposed Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. AOMDV extends the Ad hoc On-demand Distance Vector (AODV) protocol to discover multiple paths between the source and the destination in every route discovery. The message overhead in the route discovery, and route maintenance is high in AOMDV because of its on demand nature of

			routing in static topology natured WSNs.
2.	K. Guan and L. M. He	?	proposed energy-efficient multi-path routing protocol for WSNs.
		?	The route discovery mechanism provides the multiple paths between the source and destination using shared nodes in the query tree and search tree.

PROPOSED PLAN OF WORK

The secure Energy Efficient Node Disjoint Multi-Path Routing protocols (EENDMPR) protocol finds the multiple paths between the source and destination based on the rate of energy consumption and filled queue length of the node. If any node fails in shortest path then the protocol finds new shortest path from available queue instead of sending multiple request to neighbouring node like AODMVR protocol. The security threats to the WSN like spoofing or altering the route information, selective forwarding, sinkhole attack, Sybil attack and byzantine attack are removed by using the digital signature crypto system. Comparative study will be done between ad-hoc on demand multipath vector routing protocol and energy efficient node disjoint multipath routing protocol in terms of energy consumption, packet delivery fraction and end-to-end delay.

- Wireless sensor Network use Ad-hoc On Demand Multipath Vector Routing (AODMVR) protocol.

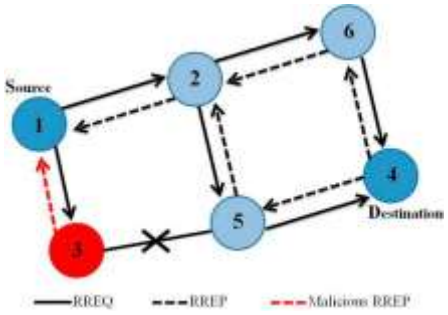
- Whenever any node fails AODMVR protocol send multiple requests to node to obtain new path.
- It increases the complexity in network hence decrease the operation lifetime of network.
- AODMVR also suffers from several security problems.
- The new approach should provide security and enhanced energy efficiency of node.
- Nodes are selected by considering threshold energy and hop count parameters.
- Sink initiated proactive protocol is used.
- The node having low energy should not be added in optimal path.
- Comparative study will be done in AOMDVR and new energy efficient approach in terms of
- Energy Consumption

BLACK HOLE ATTACK DETECTION AND PREVENTION

Black hole attacks occur when an intruder captures and reprograms a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. Black hole attack can be classified into two types

Single Black Hole Attack

As what mentioned above, a malicious node probably drops or consumes the packets. This malicious node can be regarded as a black hole problem in WSNs. Black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbours. As a result, node C is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical impact is that the PDR diminished severely. A single black hole attack is easily occurred in wireless sensor networks. An example is shown in Figure, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehaviour node who replies the RREQ packet sent from source node, and makes false response that it has the quickest route to the destination node. Therefore node A erroneously judges the route discovery process with completion, and starts to send the data packets to node C.



In the following points, different detection schemes for single black hole attack are presented in a sequential order.

Neighbourhood-based and Routing Recovery Scheme

The detection scheme uses on a neighbourhood-based method to recognize the black hole attack, and the routing recovery protocol to build the correct path In this scheme, not only a lower detection time and higher throughput are acquired, but the accurate detection probability is also accomplished [6].The neighbourhood based method is active to identify the unconfirmed nodes, and the source node sends a Modify_Route_Entry control packet to destination node to renew routing path in the recovery protocol.

Redundant Route Method and Unique Sequence Number Scheme

The first solution is to find more than one route from the source node to the destination node. In other words, there exist some redundant routes within the routing path, and assumes that there are three routes at least in the scenario.

Mohammad Al-Shurman et al. [6] propose two solutions to avoid the black hole attacks in WSN.

Time-based Threshold Detection Scheme

Latha Tamilselvan et al. [7] suggest a solution based on an enhancement of the original AODV routing protocol. It stores the packet's sequence number and the received time in a Collect Route Reply Table (CRRT), counting the timeout value based on the arriving time of the first route request, judging the route belong to valid or not based on the above threshold value. The main design concept is setting timer in the RimerExpiredTable for collecting the other request from other nodes after receiving the first request.

Random Two-hop ACK and Bayesian Detection Scheme

Djamel Djenouri et al. [8] propose a method to monitor, detect, and isolate the black hole attack in WSNs. In the monitor phase, an efficient technique of random two-hop ACK is employedAnd after a mobile node is determined that it is a misbehaviour node by the proposed detection scheme, this decision must be proved by all nodes. . The proposed Bayesian detection method does not use any periodic packets exchanging, therefore the most common overhead problem can be eliminated by this method.

Resource-Efficient ACcounTability (REAct) Scheme based on Random Audits

William Kozma Jr. et al. [9] propose a reactive misbehavior detection scheme called REAct scheme. When the performance is drop down between source and destination node, the REAct is triggered automatically. REAct constitutes of three phases: (a) the audit phase, (b) the search phase and (c) the identification phase. Then the source node chooses an audit node, and utilizes the bloom filter to create a behavioural proof. To simply describe the REAct scheme, the target node sends a acknowledge to the sender when a biggish packet drop ratio is detected. Finally, the segment location of malicious node can be distinguished from comparing the source node's behavioral proof.

Detection, Prevention and Reactive AODV (DPRAODV) Scheme

Compared to normal AODV, the RREP_seq_no is extra checked whether higher than the threshold value or not. If the value of RREP_seq_no is more than the threshold value, the sender is viewed as an attacker and added it to the black list. A new control packet called ALARM is used in DPRAODV, while other main concepts are the dynamic threshold value. Hence, the dynamic threshold value is changed by calculating the average of dest_seq_no between the sequence number and RREP packet in each time slot. According to this method, the black hole attacks not only be detected but also prevented by updating threshold which will response the realistic network environment [10].The ALARM is sent to its neighbours which includes the black list, thus the RREP from the malicious node is blocked but is not processed.

Next Hop Information Scheme

N. Jaisankar et al. [11] propose a security approach which is composed of two phases, detection and reaction. In the first phase, the field_next_hop is added to the RREP packet. Before the source node sends the data packets, the leading RREP packet is observed between intermediate node and target node. After that, the malicious node can be find out if the number of receiving packets differentiates from sending packets. The second phase is isolating the black hole, thus each node keeps an isolation table (IT) and stores the black node ID. The ID is spread to all nodes in order to eliminate the malicious node by checking the isolation table.Each node maintains a black identification table (BIT), and the fields in table are <source, target,current_node_ID, Packet_received_count (PRC), Packet_forwarded _count (PFC), Packet modified count (PMC)>. Then the PMC is updated by tracing the BIT from their neighborhoods. If the node acts properly, the corresponding count value multiplies.

Collaborative Black Hole Attack

There are various mechanisms have been proposed for solving single black hole attack in recent researches. As a result, a number of cooperative detection schemes are proposed preventing the collaborative black hole attacks. In the following points, different detection schemes for the cooperative black hole attack are presented in a sequential order. However, many detection schemes are failed in discussing the cooperative black hole problems. Some malicious nodes collaborate together in order to beguile the normal into their fabricated routing information, likewise, hide from the existing detection scheme.

DRI Table and Cross Checking Scheme

Every node needs to maintain an extra DRI table, numeric 1 represents for true and numeric 0 for false. The entry is composed of two bits, “From” and “Through” which stands for information on routing data packet from the node and through the node respectively.

Sanjay Ramaswamy et al. [12] exploit data routing information (DRI) table and cross checking method to identify the cooperative black hole nodes, and use modified AODV routing protocol to achieve this methodology.

Distributed Cooperative Mechanism (DCM)

Chang Wu Yu et al. [13] propose a distributed and cooperative mechanism viz. DCM to solve the collaborative black hole attacks. Each node in network evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node starts the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to test the cooperative node.As the nodes works cooperatively, they can analyze, identify, lessen multiple black hole attacks. In the local data collection phase, an estimate table is constructed and preserved by each node in the network. If the examination value is positive, the suspicious node is regarded as a normal node. A constrained broadcasting algorithm is used to restrict the notification range within a fixed hop count. A threshold represents the maximum hop count range of cooperative detection message. Lastly, the global reaction phase is executed to set up a notification system, and sends warning messages to the whole network. Otherwise the initial detection node starts the cooperative detection procedure, and deals with propagation and notifying all one-hop neighbours to take part in the decision making. Because the notify mode utilizes broadcasting method, the network traffic is increases. There are reaction modes in global reaction phase. Though the first reaction

mode notifies all nodes in the network, but might waste lots of communication overhead. Each node only concerns its own black hole list and arranges its transmission route in other mode, however it might be exploited by malicious nodes and needs more operation time.

Hash based Scheme

The developing mechanism is based on auditing technique for preventing collaborative packet drop attacks, such as collaborative black hole and grey hole problems[13].Weichao Wang et al. design a hash based defending method to generate node behavioural proofs which involve the data traffic information within the routing path.

Hashed-based MAC and Hash-based PRF Scheme

Zhao Min and Zhou Jiliu propose two hash-based authentication mechanisms, the message authentication code (MAC) and the pseudo random function (PRF). These two proposals are submitted to provide fast message verification and group identification, find the collaborative suspicious black hole nodes and discover the secure routing path to prevent cooperative black hole attacks.

Backbone Nodes (BBN) and Restricted IP (RIP) Scheme

This method is able to find the collaborative malicious nodes which introduce massive packet drop percentage. Vishnu K. et al. refer this method to penetrate their system model, and also add a novel scheme videlicet restricted IP (RIP) to avoid collaborative black and gray attacks. Vishnu K. and Amos J. Paul address a mechanism to detect and remove the black and gray hole attack

Bait DSR (BDSR) based on Hybrid Routing Scheme

The suggested mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major principle is the DSR on-demand routing. Po-Chun Tsou et al. design a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks.

OPEN RESEARCH CHALLENGE

Most of the previous work on WSN focused mainly on delivering packets along disjoint multipath routes such as deterministic disjoint multipath routing and randomly disjoint multipath routing. There is a need to address both these type of protocol under the attack and impact of black hole

attack on Wireless Sensor Network. . Very little attention has been given to the fact to study the impact of black hole attack in WSN using Ad-hoc on demand multipath routing protocol and energy efficient node disjoint multipath routing protocol.

CONCLUSION

Wireless sensor networks are vulnerable to wide range of security attacks because of their deployment in an open and unprotected environment. It has been studied that among the number of techniques discussed, each technique has its own strength and weaknesses and there is no proper wormhole detection technique that can detect all black hole attacks completely. This survey paper introduces the major security threats in WSN and also investigates different black hole attack detection techniques, examines various existing methods to find out how they have been implemented to detect black hole attack. Finally, by analysing the pros and cons of existing techniques, the open research challenges in the black hole detection area are studied. Presented at the 2nd International Conference on Wireless Broadband and Ultra Wide band Communications, Sydney, Australia, 27-30 August 2007

REFERENCES

1. Jamal N. Al-Karaki & Ahmed E. Kamal, (2004) “Routing Techniques in Sensor Networks: A survey”, IEEE communications, Volume 11, No. 6, Dec. 2004, pp. 6-28.
2. M. Tubaishat, S. Madria, (2003) “Sensor Networks: An Overview “, IEEE Potentials, April/May 2003.
3. Al-Sakib khan Pathan et.al,(2006) ”Security in wireless sensor networks: Issues and challenges” in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048).
4. Al-Shurman M, Yoo S-M, Park S (2004) Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE’42), Huntsville, Alabama, 2-3 April 2004.
5. Ms. Priya Maidamwar, Prof. N. A. Chavhan “A Survey on Routing Techniques for Wireless Sensor Networks”, 2012 National Conference on Innovative Research Trends in Computer Science Egg. & Technology.
6. Ms. Priya Maidamwar, Prof. N. A. Chavhan “A SURVEY ON SECURITY ISSUES TO DETECT WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK”, International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.
7. Weerasinghe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007.

8. Tamilselvan L, Sankaranarayanan V (2007) Prevention of Blackhole Attack in MANET. Paper MANETs. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6.
9. Raj PN, Swadas PB (2009) DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. International Journal of Computer Science 2:54–59. doi: abs/0909.2371
10. Jaisankar N, Saravanan R, Swamy KD (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010
11. Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in
12. Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009.
13. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.