ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Survey on Dynamic Routing in Wireless Sensor Networks under Black Hole Attack

Charulata C. Girsawale , Prof. S. A. Shirsath

Department of Communication network, SCOE, Vadgaon (Bk), Pune, India

ABSTRACT: Wireless sensor networks (WSNs) are being usedin security-basic applications. Because of theirinherent asset-constrained qualities, they are prone to different security attacks. The black hole attack is a type of attack that seriously affects information gathering. To conquer that challenge, an active detection based security and trust routing plan is proposed for WSNs. This scheme is used to detect and prevent the nodes which are affected by black hole attack. Those nodes are called as black holes. The scheme provides fair nodes for routing the data. This saves the network from losing the data.This scheme provides energy and the residual energy of black holes is used to do successful routing. The performance parameter is the energy efficiency. This is evaluated on the basis of energy dissipation while routing the data.

KEYWORDS: Black hole attack, energy efficiency, security, trust, wireless sensor network
.

I. INTRODUCTION

Wireless sensor networks (WSN) are also called as actuator networks (WSAN),are spatially dispersed autonomous sensorsto monitor physical or ecological conditions. The environmental conditions such as temperature, humidity, sound, vibrations etc. are sensed by the sensors. The sensors data is cooperatively transmitted through the system to a principle area. The improvement of wireless sensor networks was inspired by military applications such as battlefield surveillance. In present days such systems are used in numerous industrial and consumer applications such as industrial process monitoring and control, machine health monitoring and so on. A wireless sensor network can be characterized by low-size and low-complex devices. Those devices are also known as nodes in the network. These nodes are nothing but sensors in the wireless sensor network. These sensors sense the environmental conditions such as temperature, humidity, vibrations etc.

The information gathered by those sensors is transmitted in multiple hops to the sink. Sink is a centralized node in the network. The whole data is passed through this node. The architecture of WSN depends on the type of application. For a particular application the elements like nature of application, use of components, objectives, cost, hardware and architecture limitations have to be considered.

The WSN suffer from different types of security attacks. The various attacks are tampering, black hole attack, selective forwarding, Sybil attack, jamming attack, warmhole attack, and identity replication. The black hole attack is a denial of service attack. In this attack a node drops all the packets that are directed through it. This results in losing the sensitive information in the network. The main objective is to detect and prevent the black hole attacked nodes in the network. In system administration black holes refer to places in network where incoming or outgoing traffic is discarded. This happens without illuminating the source that the information did not achieve the expected beneficiary. Therefore cluster formation is used to achieve proper distribution of nodes in the network. This also provides cluster heads so that all the nodes in a cluster should communicate to others through cluster heads. This formation used to achieve detection of black holes and prevent them. By preventing them the cluster is reformed and new cluster heads are elected. The nodes do communication through those cluster heads.

II. LITERATURE SURVEY

In paper [1] a detection and prevention scheme is proposed for blackhole attack. In this scheme cluster formation is done. According to that the coordinator is responsible for checking the failure of intermediate node and detection of

DOI: 10.15680/IJIRCCE.2017. 0506167

those nodes. In blackhole attack node an intruder captures and reprogram a set of nodes in the network to block the packets. As the resultany information does not reach the destination because of high end-to-end delay and low throughput. The performance parameters of end-to-end delay and throughput are calculated under normal flow and under blackhole attack. In the presence of blackhole attack both parameters of network are affected. It degrades the performance very rapidly. The disadvantage is that the detection of blackholes is done but prevention is the area to improve. Therefore the blackholes have to be neglected from the network to save energy. This will also improve the performance parameters.

In paper [2] the network architecture consists of three layer hierarchical network architecture. Sensor nodes, access points and forwarding nodes are present in the lower layer, top layer and middle layer in the network. Thus it becomes a huge architecture. The sensor nodes are controlled by higher layer nodes i.e. forwarding nodes. The whole communication between sensor nodes is through the forwarding node. Each forwarding node has a group of sensor nodes to control them. A novel scheme based on weighted trust evaluation is proposed to detect malicious node. The forwarding node collects all the information provided by sensor nodes and calculates an aggregation result using the weight assigned to each sensor node.

$$\mathrm{E} = \sum_{n=1}^{N} W_n \times U_n (1)$$

Where E is aggregation result andU_n is sensor output. Furthermore the weightW_n of each node is kept in the range from 0 to 1.

$$W_n = W_n / \max(W_1, \ldots . . W_N) \ldots . .(2)$$

In this scheme a detection algorithm is deployed at forwarding node. If any node found dead then the architecture does not switch the cluster, it still remains in the same architecture. This is the disadvantage of the scheme. The performance is evaluated as impact of various weights on system performance and system scalability.

In paper [3] REWARD algorithm is proposed, this algorithm broadcast messages MISS and SAMBA. MISS message helps to identify malicious nodes. SAMBA helps to find physical location of the malicious node. While detecting the malicious node in the network, a MISS (material for intersection of suspicious sets) message is send to another node. When destination receives the query, it sends its location back and waits for a packet. If the packet does not arrive within a specified time then the node is considered as blackhole attacked node. After five transmissions, the destination receives 2 packets with identical data. Each nodes transmission are directed to the immediate neighbor, one node backward and one node forward. If any node drops the packet then it will be detected by next node in the path. The sender waits for predefined time period, transmits the packet changing path and broadcast SAMBA (Suspicious area mark a blackhole attack) message. This provides physical location of blackhole attacked nodes. For the proposed algorithm more energy is drawn from the batteries of involved nodes. REWARD can detect attacks by M no. of black holes require energy described by following equation,

$$E = A(M \times d)^n + (M + 1)E_R + M \times E_c \qquad (3)$$

Where A is proportionality constant, E_R is energy for receiving, E_c is energy for computation and d is the distance between source and destination. The energy is calculated and blackholeattacked node is detected. The performance parameter is the energy overhead. The method is for detection and preserving the packet to transmit through malicious nodes. This routing algorithm is energy consuming.

In paper [4] the cooperative black hole attack is prevented. The solution proposed good performance in terms of throughput, packet loss percentage, average end-to-end delay and route request overhead. There are mainly three protocols in Ad-hoc networks, Ad-hoc on demand destination vector [AODV], Dynamic source routing [DSR], Destination sequence distance vector routing [DSDV]. From those AODV is a vulnerable to black hole attacks. The source node broadcast a RREQ (route request) to discover the secure route. The nodes which reply to that message will be considered as nodes of secure route.Each performance parameter is calculated as following equations.

A. Throughput Ratio

$$T = \frac{\sum_{i=1}^{n} T_i^r}{\sum_{i=1}^{n} T_i^s} \times 100 \qquad (4)$$

Where T_i^r is the average receiving throughput and T_i^s is the average sending throughput for the i^{th} application and n is the number of applications.

B. Packet Loss Percentage

Data packet loss rate, L is calculated as follows,

$$L = \frac{\sum_{i=1}^{n}(N_i^s - N_i^r)}{\sum_{i=1}^{n} N_i^s} \qquad (5)$$

Where N_i^s and N_i^r are the number of application data packets sent by the sender and the number of data packets received by the receiver respectively for i^{th} application and n is the number of applications.

C. Average end-to-end delay

Average end-to-end delay is denoted as D,

$$D = \frac{\sum_{i=1}^{n} d_i}{n} \, (6)$$

Where d_i is the average end-to-end delay of data packets of i^{th} application and n is the number of CBR applications. Through this technique the black hole attacked nodes can be neglected from the route but the source node has to broadcast the packet every time while routing the data. This consumes more energy.

In paper [5] a cluster based hierarchical trust management protocol for wireless sensor network to deal with malicious nodes is proposed. There are two level of hierarchy in which one is sensor node and other is cluster heads are present. This protocol conducts peer-to peer trust evaluation between sensor nodes and cluster heads and trust update interval is Δt. These two level of peer-to-peer trust evaluation process four different trust components are considered. Those are intimacy, honesty, energy and unselfishness. The following equation shows peer-to-peer trust evaluation,

$$T_{ij}^{X}(t) = \begin{cases} (1-\alpha)T_{ij}^{X}(t-\Delta t) + \alpha T_{ij}^{X,direct}(t), \\ \quad if\ i\ and\ j\ are\ 1-hop\ neighbors; \\ avg\{(1-\gamma)T_{ij}^{X}(t-\Delta t) + \gamma T_{ij}^{X,recom}(t)\}, \\ \quad otherwise \end{cases} \ldots\ldots.(7)$$

When a node I evaluates a trustee node j at time t, it updates $T_{ij}^{X}(t)$ where X indicates a trust component. In the above equation $T_{ij}^{X,direct}(t)$ is the trust based on direct observations and $T_{ij}^{X,recom}(t)$ is the trust based on past experiences. Δt is the trust update interval toward node j to update $T_{ij}^{X}(t)$. The parameters α and γ are used to weigh trust based on direct observations and recommendation vs. past experiences.

The trust based intrusion detection algorithm then develop a statistical method to access trust based IDs (intrusion detection) based on selecting a system minimum threshold below which a node is considered as compromised and should be neglected. The performance comparison between weighted summation and data clustering algorithm is done. The comparison is based on false positive probability and detection probability. The results indicate trust based geographic routing protocol performs close to ideal performance of flooding based routing. The disadvantage of this scheme is that it is not energy efficient and for routing more energy is consumed.

In paper [6] check agent technique is used to detect the black holes. It is a software program in Java language which is self controlling and it moves from node to node for checking whether it is a black hole or not. When check agent visit a node, it checks the frequency of receiving packets for every neighboring node in the list of nodes. If it finds 0 for neighbor node then it doubts node is a black hole node and it triggers routing process algorithm through multiple base stations for time Δt.This technique uses routing through multiple base stations only when there is a chance of occurrence off black holes in network. The parameters like number of nodes, no. of base stations, no. of black hole nodes and no. of check agents are considered. The performance parameters average energy of nodes and packet delivery ratio are evaluated. The average energy of nodes at every time instances is evaluated. Similarly the packet delivery ratio is considered for observing successful routing.

In paper [7] black hole attack detection and prevention technique is used. The proposed black hole detection and prevention scheme uses fuzzy logic algorithm. The multiple base stations are used to improve the data delivery. This multiple base station receives the same packet. After detection of black holes in the network, those nodes are removed and network is reformed. The performance parameters like total drop packets, routing overhead, packet delivery ratio, actual packet loss are considered. Those parameters are checked before and after black hole attack. These parameters help to determine the consequences of black hole attack effectively on the wireless sensor network. This is not an energy efficient scheme.

In paper [8] an exponential trust based mechanism is proposed to detect malicious node. In this method a steak counter is deployed to store the consecutive number of packets dropped and a trust factor is maintained for each node. The trust factor decreases exponentially with each consecutive packet dropped which help in finding malicious node. The method shows a huge decrease in the number of packets dropped before detecting the node as malicious node. In the exponential trust based mechanism, the concept of overhearing which was proposed in watchdog technique. The overhearing task is performed by cluster heads. A streak counter is maintained to count consecutive number of packets dropped by any node. When the trust factor goes below a given threshold value then the node is considered as black hole attacked node. After the detection of dropped packets, those packets are retransmitted. The performance of the proposed mechanism is evaluated on the basis of trust factor vs. no. of packets dropped. The graph of trust factor vs. no. of packets drop is exponential in nature. The mechanism gives information about the no. of packets dropped in the network but exactly how many nodes are attacked in the network is not considered. As well as the prevention is also not a subject of concern.

In paper [9] for various attacks an efficient detection of attack techniques are discussed. The trustworthiness of node is checked, whether they behave maliciously or not. Nodes with low trustworthiness are then avoided during routing decision. The behavior of nodes is decided on the basis of packet forwarding, remaining energy, network layer acknowledgement and authentication. The malicious nodes are spread all over the sensor network for detecting them weigh value is used. For the parameters like packet forwarding, network acknowledgement, integrity, authentication, confidentiality and energy. The weigh values are 0.3, 0.2,0.2, 0.1, 0.1 respectively. According to that black holes are detected. For each trust parameter except remaining energy source node calculates destination node based on following equation,

$$T_i^{s,d} = \frac{S_i^{s,d}}{S_i^{s,d}+F_i^{s,d}} \qquad (8)$$

Where S_i and F_i stands for the number of successful and failed co-operations between source and destination respectively. To perform routing decision weighted routing cost function which incorporates the trust information through the following equation,

$$W(T) * T^{s,d} + W(D) * D^d \qquad (9)$$

Where D^d is the distance metric equal to one minus the relevant distance between destination and source, compared to the sum of distance of all one hop neighbors. The node that is closes to the destination maximizes D^d.In this method giving weighted values decides black holes in the network but prevention of those is not considered.

In paper [10] proposes a mechanism which provides secure route discovery for the AODV protocol (SRD-AODV) to prevent black hole attack. The Route Request (RREQ) and Route Reply (RREP) message are used to establish connection between source and destination nodes. AODV is a reactive routing protocol that generates route through network when communication begins. Each node has sequence number. As link changes sequence number increases. For the discovery of secure route threshold of nodes are defined. On the basis of them whether the node is black hole attacked or not is decided. If these types of nodes send any RREQ then it is discarded. The maximum (MIN) and minimum (MIN) sequence number (SEQ).

$$MIN_{SEQ} = 0$$

$$MAX_{SEQ} = 4294967295$$

The parameter threshold is considered for the node.The threshold is classified for three types of environment small, medium, large. For small, medium and large environment threshold is defined by following equations,

$$TH_s = \frac{MAX_{SEQ}\times 94}{100} \qquad (10)$$

$$TH_M = \frac{MAX_{SEQ}\times 96}{100} \qquad (11)$$

$$TH_L = \frac{MAX_{SEQ}\times 98}{100} \qquad (12)$$

The performance parameter is the packet delivery ratio. The simulation results show that SRD-AODV mechanism greatly increases the packet delivery ratio with node mobility when black hole attacks are occurring on the network. In this mechanism, the connection to every node is not there and for every communication RREQ request is broadcasted which energy consuming as well. The cluster formation is also not provided for proper communication.

III. CONCLUSION

Various types of routing algorithm and methods are reviewed. The performance parameters like throughput, packet delivery ratio, end-to-end delay, energy and packet drop are discussed. The trust based mechanism for detection and prevention of black holes are elaborated. In trust based mechanism peer-to-peer trust evaluation is much better because it evaluates for a node as well as for neighboring node. The performance is shown in the form of probability of compromised node. For detection of block holes cluster coordinator technique is efficient. Because the parameter like throughput, packet delivery ratio and end-to-end delay is evaluated by the black hole attack detection and prevention technique. The cluster coordinator also keeps the record of it for successful routing. After detection, prevention of the black holes is important. The cooperative black hole prevention algorithm enhances in terms of packets loss, throughput and end-to-end delay. The prevention of black holes is done by secure route discovery which increases packet delivery ratio.

REFERRENCES

[1] M. Wazid, A. Katal, R. Singh Sachan, R. H. Goudar, D. P. Singh "Detection And Prevention Mechanism For Blackhole Attack In Wireless", IEEE International Conference On Communication And Signal Processing (ICCSP), 3-5 April 2013.

[2] M. Atakli, H. Hu, Y. Chen, W-S. Ku, Z. Su "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", In Proceedings Of The 2008 Spring Simulation Multiconference. Society For Computer Simulation International, pp 836-843.

[3] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor", Wksp. Real-World Wireless Sensor Networks June 2005, pp 20-21.

[4] Hesiri Weerasinghe, Huirong Fu, “Preventing Cooperative Black Hole Attacks in Mobile Ad HocNetworks: Simulation Implementation and Evaluation”, IEEE International Conference On Future Generation Communication And Networking, 6-8 December 2007.

[5] Fenye Bao, Ing-Ray Chen, Moon Jeong Chang and Jin-Hee Cho, “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection” IEEE Transactions On Network And Service Management, Vol. 9, No. 2, June 2012.

[6] Nitesh Gondwal, Chander Diwaker, “Detecting Blackhole Attack In Wsn By Check Agent Using Multiple Base Stations”, American International Journal of Research in Science, Technology, Engineering & Mathematics,Vol. 3, No. 2, June-August, 2013, pp 149-152.

[7] Jaspreet Kaur , Bhupinder Kaur, “BHDP Using Fuzzy Logic Algorithm For Wireless Sensor Network Under Black Hole Attack” , International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, No.9 ,2014, pp 142-151.

[8] Dr. Deepali Virmani ,Manas Hemrajani , Shringarica Chandel ,” Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network”, arXiv preprint arXiv January 2014, pp 1401-2541

[9] Theodore Zahariadis, Panagiotis Trakadas, Sotiris Maniatis, Panagiotis Karkazis, Helen C. Leligou, StamatisVoliotis, “Efficient detection of routing attacks in Wireless Sensor Networks”, IEEE 16th International Conference on Systems, Signals and Image Processing, 18 June 2009, pp 1-4.

[10] Keecheon Kim ,Seryvuth Tan ,”Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs ”, IEEE International Conference On ICT Convergence, 14 October 2013, pp 1027-1032.