Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.822 – 828

RESEARCH ARTICLE

Black Hole Prevention & Detection under Average Energy Consumption in WSN

Rajni Rani
Ms. Preethi Dolly, HOD in CSE dept.
Mr. Devender Kumar, Assistant professor in CSE dept
Meri College of Engineering & Technology Sampla, Haryana, India

ABSTRACT

Wireless sensor networks are mostly maddening in some applications related frontline monitoring. The study of selecting cluster heads by the sink is based on the minimization of the related additional energy and residual energy at each node. In our proposed work, the intermediate node selects the near neighbor distance and higher energy sensor node to transmitted the packet, if there more than three packet transfer at the same clock so that flooding would be occur to reach the sink between the direct approach and the indirect approach with the use of the nearest cluster head so it block the packet transmitting path behind of black hole region so we preventing such as Average Energy consumption with min Distance vector and minimize dead node occurrence.

Keyword: Black hole, WSN, SEP, BSEP, PACKET, RESPONSE

INTRODUCTION

The security is the leading matter in WSN due to the control of the computational volume and power usage. Wireless sensor network has much robust and active methods of Security to device the attacks caused by the malicious nodes in the network.

Later Earlier research on wireless sensor network displays that they are new susceptible to attacks than static networks. Hence, some security explanations that are appropriate for static packet transfer network but don’t work fine on wireless sensor network. Several of the attacks caused by the malicious nodes are wormhole attack, Black hole attack, gray whole attack, and denial of service, hello flood attack, Sybil Attack and Selective Advancing attack and numerous more attacks.

AODV is Ad-hoc on-demand Multipath Distance Vector (SEP) packet transfer protocol which is used for the multiplying multiple loop-free and connection separate paths. For every endpoint, end to end with the respective hop sums it covers a gradient of the packet transfer accesses of the next-hops. Similar sequence number is billed to all following hops. This supports for observance path of a route.

A node preserves the allocated hop count, which is the extreme hop total for all the paths at every node. Loop freedom is certain for a node by tolerant alternative path to destination if it has a less number of hop totals than the allocated for that destination. SEP permits intermediary nodes to reply to Flooding, where as stagnant choosing splits paths.

Throughout route discovery, its message overhead is high, owing to amplified flooding. Subsequently it is a multipath packet transfer protocol; the destination answers to the multiple Flooding those results are in longer overhead.

The main packet transfer protocols are of 2 types i.e. Protocol operation type and Network structure type. . Packet transfer protocols are considered to gratify mission such as collision circumvention or prevention and faster data broadcast. So that energy efficiency and low latency can be succeeded. The two protocols deliberated here are SEP and BSEP and are compared in Result sections.

LITRATURE REVIEW

Virmani et al. (2014) proposed an exponential trust based mechanism to detect the malicious node. In this method a Streak counter was deployed to store the consecutive number of packets dropped and a trust factor was maintained for every node. The trust factor drops exponentially with every consecutive packet dropped which helps in detecting the malicious node. The method showed a drastic decrease in the number of packets dropped before the node being detected as a malicious node. [1]

Baviskar et al. The security in wireless sensor network is a main issue due to the limitations of power usage. Several techniques based on secret sharing and multi-path packet transfer have been proposed in it However, these techniques are not very effective, and when demonstrate, they may even end up making black hole attacks more effective. Propose an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission and performance compare with multiple base stations and without multiple base station to prevent black hole attack. [2]

Wazid et al. proposed an algorithm used for detection and prevention of black hole attacks which is harmful for the wireless sensor networks. Black hole is just like as DOS attack. Black hole attacks degrading in the performance of network parameters are affected *i.e* end- to- end delay and throughput**.** [3]

Dighe et al. proposed a technique based on secret sharing and multipath packet transfer to overcome black hole attacks in the network. However, these techniques were not very effective. The efficient technique that uses in multiple base stations deployed in the network to reduce the impact of black holes on data transmission. [4]

Wazid et al. Proposed the comparative performance analysis of two WSN’s topologies i.e. Tree and Mesh under black hole attack is done. If there is a WSN prone to black hole attack and requires time efficient network service for information exchange then Tree topology is to be chosen. If it requires throughput efficient and consistent service in the network then Mesh topology is used. An algorithm named as Topology Based Efficient Service Prediction (TBESP) algorithm was proposed depending upon the analysis done which will helped in choosing the best suited topology as per the network service requirement under black hole attack. [5]

Problem Statement

Before the mechanism complete on WSN absorbed mostly on dissimilar security threats and attacks such as DoS, DDoS, and Impersonation, Wormhole, Jellyfish, and Black Hole attack. Amongst these attacks Black Hole attack elaborate in WSN is assessed founded on reactive packet transfer protocol comparable Ad-Hoc On Demand Distance Vector (AODV) and its properties are expanded by declaring how this attack disturb the performance of WSN. Actual slight devotion has been assumed to the detail to revision the impression of Black Hole attack in WSN using both Reactive and Proactive protocols and to associate the susceptibility of both these protocols contrary to the attack. There is a need to statement together these types of protocols below the attack, as well as the impressions of the attacks on the WSNs. This Research examines Black Hole attack in WSN using SEP& BSEP which are reactive respectively in nature.

PROPOSED IMPLEMENTATION

In the BHDPT (black hole detection & prevention technique) using SEP& BSEP algorithm

Phase 1: Create a wireless sensor network of N nodes

Phase 2: Explain the member nodes of one BS (Base station) according to given range

Phase 3: select the neighbor member of nodes which is neighbor to the base station

Phase 4: send the packets from one node to another node

Phase 5: Analysis the parameter such as end to end, packet transfer overhead, total energy consumption, Throughput for each nearest node

Phase 6: Apply BSEP to do detect under the network under black hole attack or not

Phase 7: Remove the attack

It is considered that if the residual energy of a node is greater than the average residual energy of the network, then this node has sufficient energy and has a high probability of transmitting more data packets before being exhausted.
This case corresponds to ($w(u_j) \geq \beta$),

so:$\beta = e_{\mathrm{averageNet}}(P(u_0,u_n))$……………………….1

Therefore, $T_{\mathrm{Net}} = \prod_{j=1K} \alpha * w_{(u_j)\beta} \leq a_k$, and we obtain the following:

$\alpha \geq (T_{\mathrm{Net}})_{1/K}$ ……………………………………………..2

Following Equation 1, we obtain

$\alpha < \beta_{w(u_j)}$ …………………………………………….3

steady-state probabilities can be solved.

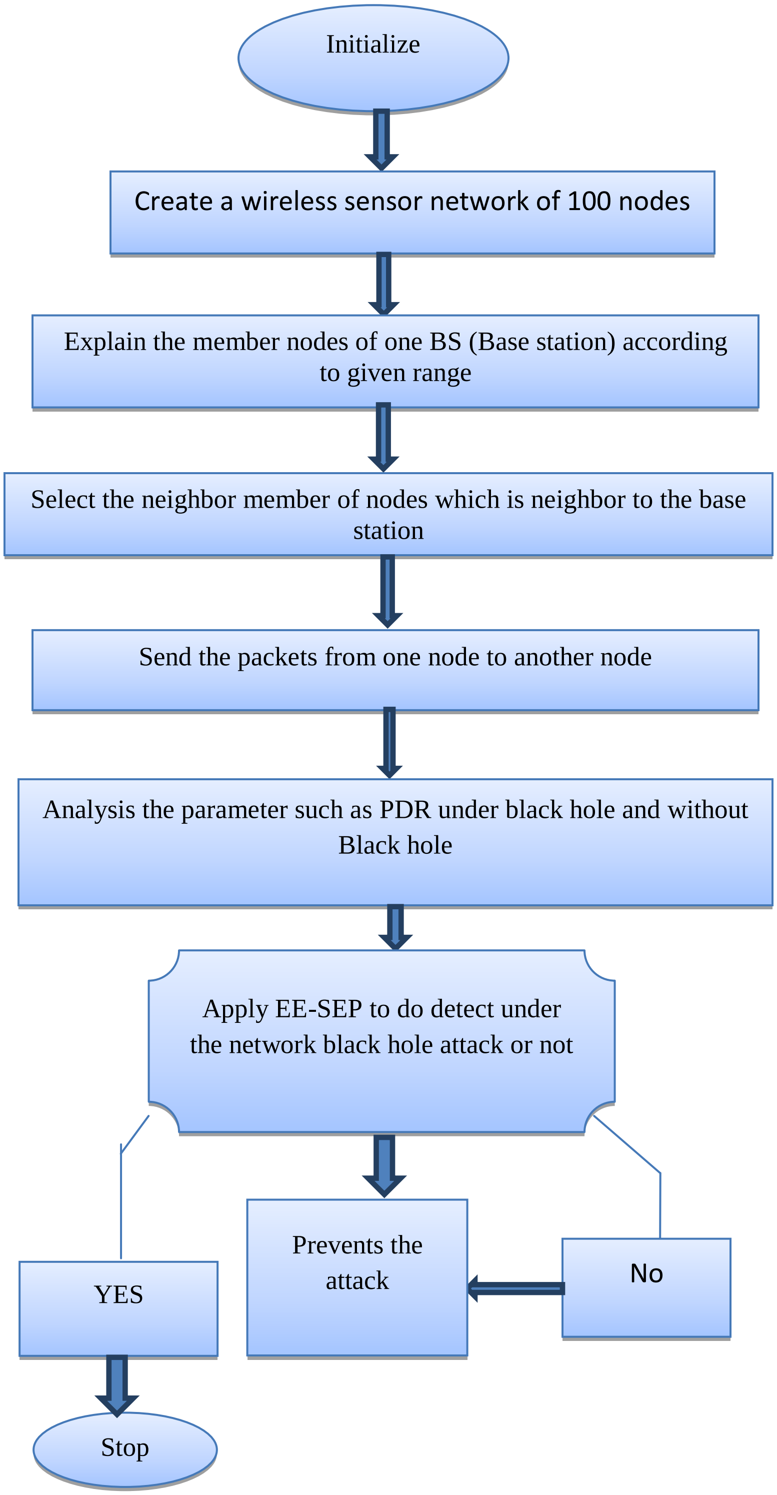
Initialize
Create a wireless sensor network of 100 nodes
Explain the member nodes of one BS (Base station) according to given range
Select the neighbor member of nodes which is neighbor to the base station
Send the packets from one node to another node
Analysis the parameter such as PDR under black hole and without Black hole
Apply EE-SEP to do detect under the network black hole attack or not
YES
Prevents the attack
No
Stop

Figure 1: Proposed Flow Diagram

To solve the value of steady-state probabilities, transition probability values are given as the following: pa = 0.4; pm = 0.3; pe = 0.5; pi = 0.6.'

By solving equations (3) and (1), steady-state probability values can be computed as: vG=0.3333, Vv=0.3333, va=0.1333, Vuc=0.0267, vMc=0.0400, vd=0.0667, vgd=0.0400, Vf=0.0267.

RESULT

The SEP protocols are implemented using MATLAB2012a software to activate network. The performance of using T-SEP protocols are associated with and deprived of multiple based stations on numerous network parameters.

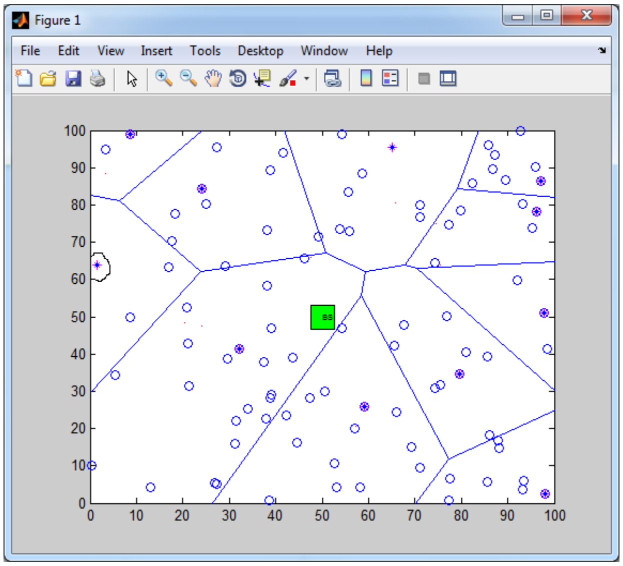

Figure 2: Blakhole detection at unbound distance from one zone to another zone

Figure 1shows the exact locations of the black holes in the WSN network. The first malicious node forwards the packet using the compulsory communicate power to deceive two nodes backward. The second malicious node drops the packet; though the attack is detected by the last node earlier the black holes. The missing transmission is shown by a circle line in Figure 1.

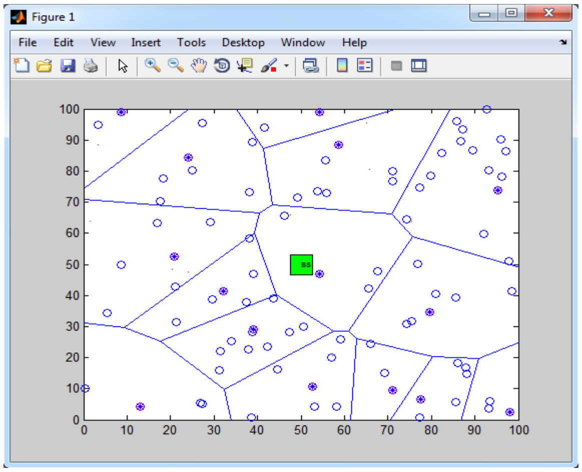

Figure 3: Blakhole prevention by SEP

In a WSN, effective packet delivery to the BS is more basically compulsory than the prevention of data to be taken by an attacker.

By using efficient SEP anonymity techniques, the information seized by an attacker can be completing insignificant. So, focus should be on the objective of delivering the packets to the BS in the presence of black hole nodes.

Here, a good solution is proposed that uses multiple BSs located in the network to improve the delivery of packets from the SNs reaching at least one BS in the network, thus confirming high packet delivery success

```
node 1 sends PACKET Secure Multipath to node 3

node 1 sends PACKET Secure Multipath to node 4

node 1 sends PACKET Secure Multipath to node 5

node 1 sends PACKET Secure Multipath to node 7

node 1 sends PACKET Secure Multipath to node 8

node 1 sends PACKET Secure Multipath to node 9

node 1 sends PACKET Secure Multipath to node 14

node 1 sends PACKET Secure Multipath to node 15

node 1 sends PACKET Secure Multipath to node 16

node 1 sends PACKET Secure Multipath to node 17

node 1 sends PACKET Secure Multipath to node 20

Flag= 1

 Node 20sends RESPONSE  to node 1

 Node 1 Sends message to node 20
```

Packet transfer in T-SEP&SEP Protocols: From the graph, it has been seen that for 100 nodes, packet delivery ratio is large in compare to other two protocols where it is less in AODV compare to but T-SEP has larger packet delivery ratio compare to BSEP protocol.

CONCLUSION

In this paper we have executed the route discovery using SEP protocol. SEP establishes multiple loop-free and link-disjoint paths. Our research we conclude that AODV protocol is more vulnerable and in a network any black hole detected the anchor node should not be acquire the position if any anchor node will acquire the position the same network black hole cant not be exist there that will improve black hole region attacks is black hole attack. The results of simulation show that this attack has high effect on SEP protocol. In this case, based on the number of attacker, the Packet Delivery Ratio is high. If the number of them increases, the Packet Delivery Ratio is low, because we have black hole attack.

REFERENCES

[1] Dr. Deepali Virmani,, Manas Hemrajani and Shringarica Chandel., "Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network " Bhagwan Parshuram Institute of Technology,vol.1 Jan(2014).

[2] B.R. Baviskar and V.N.Patil "Black hole Attacks Prevention in Wireless Sensor Network by Multiple Base Station Using of Efficient Data Encryption Algorithms" International Journal of Advent Research in Computer & Electronics, Vol.1, No.2, (2014).

[3] Mohammad Wazid , AvitaKatal ,Roshan Singh Sachan , R.H Goudar and D.P Sing., "Detection And Prevention Mechanism For Black hole Attack" in Wireless Sensor Network IEEE,(2013)

[4] Pranjali G Dighe , and Milind B Vaidya "Counter Effects of Black Hole Attack on Data Transmission in Wireless Sensor Network with Multiple Base Stations" International Journal of Engineering and Innovative Technology (IJEIT) Vol.3,Issue5, (2013)

[5] Mohammad Wazid, AvitaKatal, Rooshsn Singh, Sachan , R.H Goudar and D.P Singh, "TBESP Algorithm for Wireless Sensor Network Under Black Hole Attack" IEEE International Conference on Communications (ICC) (2013).

[6] Bo-Chao Cheng, Hsi-HsunYeh, and Ping-Hai Hsu"Schedulability Analysis for Hard Network Lifetime Wireless Sensor Networks With High Energy First Clustering" 2011 IEEE.

[7] M.K.Marina and S.R.Das, "On-Demand multipath distance vector packet transfer in ad hoc networks" in: Proceedings of the 9th IEEE International Conference on Network Protocols (ICNP), 2001. http://www.elec.qmul.ac.uk/research/thesis/XuefeiLi2006-thesis.pdf.