Biomedical Research 2016; Special Issue: S204-S209

ISSN 0970-938X
www.biomedres.info

Detecting and preventing black hole and wormhole attacks in wireless bio sensor network using path assignment protocol.

Manikandan KP[1]*, Satyaprasad R[2], Rajasekhararao K[3]

[1]Department of Information Technology, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamil Nadu, India

[2]Department of Computer Science, Achariya Nagarjuna University, Andhra Pradesh, India

[3]Sri Prakash College of Engineering, Rajupeta, Tuni, Andhra Pradesh, India

Abstract

Many networks are available for coruscate secure communication on the wired, wireless, and ad hoc networks. The Central Network Authority Infrastructure (CNAI) is moving towards a new domain of communication such as Wireless Bio Sensor Network (WBSN), perhaps any node communicate with inter or intra region's nodes, the chance to dissemble the packet, route and medium (source and destination). Moreover, other than wired, wireless networks, the WBSN is full of security challenges. For instance, the vulnerability of attack in the form of black hole and wormhole is causes the packet delivery between the medium of CNAI. These causes bring down the secure communication, to blow up drawbacks of security in WBSN, the attacks deduction and reduction is essential. Therefore this paper proposes a rapid response round trip time mechanism to detect the black hole and wormhole attacks. In addition to this, the path assignment protocol used to reduce those attacks and produce the higher efficiency and throughput with cost-effective.

Keywords: Central network authority infrastructure, Wireless bio sensor network, Rapid response round trip time, Path assignment protocol.

Accepted on August 31, 2016

Introduction

Due to the advancement of wireless communication and sensor technology, have ensuring the security of the network is extremely important. There are several limitations associated with biosensor networks such as limitation in power, memory, computation capability, and communication rate which makes the wireless biosensor security a real challenging problem. A body biosensor network is a group of wireless sensor nodes used to measure biological parameters which can provide valuable medical information [1]. Presence of malicious node in the WBSN networks that arisen many attacks such as black hole [2] and wormhole attacks. In this paper we propose the Path Assignment Protocol, it communicate and detect the attacks on the each node and forward data packets by using it. Both attacks are vulnerable against an on routing path especially in the Dynamic Source Routing (DSR) [3] or Ad hoc On-Demand Distance Vector (AODV) protocol [4] are generally used protocol for forming the secure route against attack and prevent the discovery [5] of any routes by reducing overhead and improve the scalability and resilience to node. To find the black hole [2,6] and wormhole attack [7] on the WBSN, proposed system consists of three considerations. Firstly, watching the transmission time between the malicious nodes to detect the suspicious node transmission by using rapid response round trip time (R3T2), which is useful to detect the initial stage of the attack detection by comparison of history behind the transmission, whether the process takes the higher time or lower time of node packet delivery with un-suspicious nodes. Secondly, we introduce the Path Assignment Protocol (PAP) for finding the distance [8] between the suspicious nodes, which is useful to count the nodes available between the medium. Thirdly, to reduce both round trip time and new path of the nodes are reduced so attacks are also reduced by based on the threshold based wormhole [7,9] and black hole detection [2,10] in WBSN. An experimental result shows that the proposed method achieves high network performance in terms of throughput and packet delivery ratio and so on.

Problem Definition

To design the WBSN as the high transmission delivery time and low communication overhead for secure communication. The rapid response round trip time used to malicious nodes to detect the suspicious node by using the transmission time consideration. To develop the efficient protocol for path detection [10] for the shortest distance for packet delivery [8]. The Path Assignment Protocol used to the find the shortest path between the two nodes. To maintain the accurate detection of the severe attacks such as block hole [7] and wormhole attack [7,9]. The threshold based method used to detect wormhole and black hole attacks.

Research Methods

Rapid response round trip time (R3T2)

The rapid response round trip time are measured for calculating the response time and reply time of the node for find the shortest time interval. The three sections are available in timeline flow of rapid response round trip time namely timeline flow for rapid response round trip time, normal node RRep (T) and nearest neighbour node selection [11,12]. Those section are regular calculate the time taken for the packet delivery and the reply sequences.

Timeline flow for rapid response round trip time

The each sender and receiver is communicated each other with respect to the intermediate nodes. The sender node is send the request $(R_{Req})_S$ to I1 message to the nearby nodes likewise the $(R_{Req})_S$ to I2, $(R_{Req})_S$ to D are send from the intermediate node I1 and I2 respectively to the destination. At the same time the response from destination to the respective sources are managed with the time interval.

Normal node RRep (T)

The request and response time were taken and stores in the past interaction history (The past transaction history) for the future reference, this history of node transmission are used compare the any transmission delivery time with the new time interval between the two distinct source and destination.

The past transaction history contains the node identification number and gateway to interface node and the metric value for the current communication. If the packet sends over the network from two different nodes, the history of the source routing, hop-by-hop routing, and routing metric is stored in past transaction history. If any routing path exists while packet sending over nodes, the packet did not send that route because of the two reasons that firstly, the route is already patterned secondly, the route has some malicious attacker and also gives the delay of intruder, control overhead, packet delivery ratio, energy consumption, queue delay and agent trace of the overall networks. The analysed values are modelled by the following formulae which are used to find the correct route path of any nodes. In addition to that the attackers are finding based on the trust values.

Number of itration on the same path=Number of nodes presented in the MN*cost metrices

Number of route on the gateway=number of gateway between the two nodes/current number of nodes to gateway interfaces

Equations give the general past interaction history it will direct to the find the number of nodes are presented and in the form of attacker.

The analysed values of past interaction history constructed in the Table 1 which is useful to find and combine the number of iteration and number of route in the concern network nodes. This is used to store the previous history of the normal scheme in Wireless Sensor Networks (WSN).

Nearest neighbour node selection

The nearest neighbour node selection [11] is useful to find nearest neighbour node based on route source and destination node [12]. The similar to the rapid response round trip time request and reply the nearest node has been calculated based on the with respect to the sender request packet and receiver reply message with respect to the two distinct node.

This is extended nearby shortest node. Each process contains the transmission time which is stored for the comparison process. This transmission record is compared with the normal node RRep (T) for transmission finding the attack like wormhole. The recorded time consumption is compared with the Table 1. This variation is given as the attacks or malicious are formed with the tunnelling. The tunnel values of the each source and destination is discovered as the warm whole attack.

Table 1. *General past interaction history.*

Network Id		Next hop	Current node to gateway	Cost	No of nodes presented	No iteration of same path	No. of. Route
Network destination	Net mask	Gateway	Interface	Metric			
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.100	10	126	1260	2
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	16382	16382	7
192.168.0.0	255.255.255.0	192.168.0.100	127.0.0.1	10	100	1000	1
192.168.0.100	255.255.255.255	127.0.0.1	127.0.0.1	10	27889	278890	11
192.168.0.1	255.255.255.255	192.168.0.100	192.168.0.100	10	27734	277340	11

Where threshold (t) is varied from the $(0<t \leq 1)$ for choose the t is higher than 0 the delay is low, therefore the black hole attacks [2] are discovered else the delay is high the wormhole attacks are discovered from the mobile ad hoc network. Moreover path assignment protocol is used to find the distance

[8] between the suspicious nodes by the route path between them.

$$Wormhole\ RRRTT_{Before\ attack} = \sum\nolimits_{node\quad 1}^{n-1} (ReqT - ResT)_n$$

$$Wormhole\ RRRTT_{After\ attack} = \sum\nolimits_{node\quad 1}^{n-1} (tRRRTT - \ (1 - t_{RRRTT}))_n$$

Path assignment protocol (PAP)

The proposed Path Assignment Protocol (PAP) consists of hybridization of two routing protocol such as zone routing protocol and zone-based hierarchical link [13] state protocol which is used to reduce the route discovery overheads between the suspicious nodes [5]. In Path Assignment Protocol, works based on the combination of zone routing protocol and zone-based hierarchical link [13] state routing protocol, both the routing protocol are hybrid protocol which works based on the proactive as well as reactive routing approaches which is used to reduce the control overhead and latency. In addition to this the inter-zone and intra-zone routing packets are used to finds nearest neighbour nodes [11] between the n neighbours in the mobile ad hoc network [12] which is described as in Figure 1.

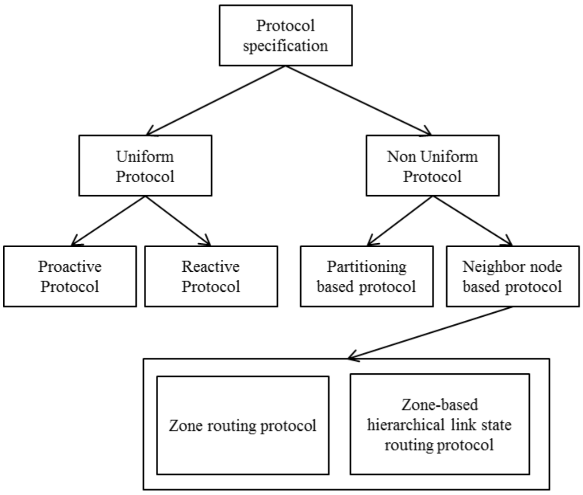

Figure 1. *Proposed protocol specification.*

Consider the number of hop in the network zone, all nodes counted as the n1, n2, n3 and so on commonly N. Particularly the routing zone described as routing edge peripheral nodes of N are N's neighbouring nodes [11] in its routing zone which are exactly d hops away from N this routing called as the Zone routing protocol. We combine this routing protocol with zone-based hierarchical link state by form the zone as hierarchical structure with respect to the neighbourhoods N as node level topology [11] and zone level topology, which is reduce the within multiple overlapping zones in the Zone routing protocol. This non-overlapping zones are formed the location management where reduce the data transmission energy of the cluster-head or location manager when data transmission between the two nodes. To improve the efficiency of the route finding by the reduction of overlapping, sequentially changing of variable size zones, those parameters are used to manage the Zone Routing Protocol (ZRP) with the Zone-Based Hierarchical Link State (ZHLS). This hybrid routing topology path assignment protocol used to find the path distance [8] based on the node ID and the zone ID of the destination is required for routing. The proposed hybrid routing protocols named path assignment protocol has potential to provide higher scalability than pure reactive or proactive protocols for insignificant to reduce the number of retransmission of the nodes applicable to routing. By working together the best or the most suitable nodes can be used to perform route discovery [5]. The nodes within each zone work together to maintain location information about the nodes which are assigned to that region. This is potentially eliminated the warm hole and black hole, by the novelty of hybrid routing protocols of path assignment protocol.

Results

The WBSN environment is formed by using NS2, which consist of wireless nodes with the simulation setting such as simulation area, simulation time and simulation sources. The different types of attack such as black hole, wormhole are detected [9] based on the malicious nodes appear in the simulation setting and affect the same. Our proposed system aim is to show that path assignment protocol performs better than many existing method like SETX, ENCBTS-colluded ABH, AM and so on. Conclusions are drawn for the black hole attack, wormhole attack are reduced by the following network setup. The standard network simulator 2 used for mange and demonstrates dynamic nature of mobile ad hoc [14] networks and the performance evaluation are compared with the various parameters with various protocols by following simulation parameters given in Table 2.

Table 2. *Simulation parameters.*

Routing protocol	Path assignment protocol
Number of nodes used for sample	40
Number of nodes as black hole nodes	2
Number of nodes as wormhole nodes	4
Mobility speed	10 mps
Simulation time	120 sec
Simulation area	1000*1000 m^2
Transmission range	300 m
Mobility movement	Random path
Transmission rate	2 packets/seconds
Connections count	25 connection
Number of source nodes	3

Target node	All nodes in the Simulation area
Buffer size	250 packets

To evaluate the performance of the proposed method, we compared proposed protocol with the standard existing protocols under a wormhole and black hole attack [2,15] on the network. The performance matrix of simulation is based on the mobility speed with respect to the packet delivery ratio, packet loss rate, detection ratio [16] in the simulation scenario are described in the following Figures.

Packet delivery ratio

Packet delivery ratio defined as ratio between the numbers of packets successfully received at the destinations and total number of packets sent by the sources and the number of delivered data packet to the destination illustrates the level of delivered data to the destination. Mathematically, it can be defined as follows,

Packet delivery ratio=(packets received/packets delivered) × 100

Here delivered packets are defined as number of successfully delivered packets to the destination. Figure 2 illustrate the scenario of packets delivered to destination in black hole and wormhole attacks.

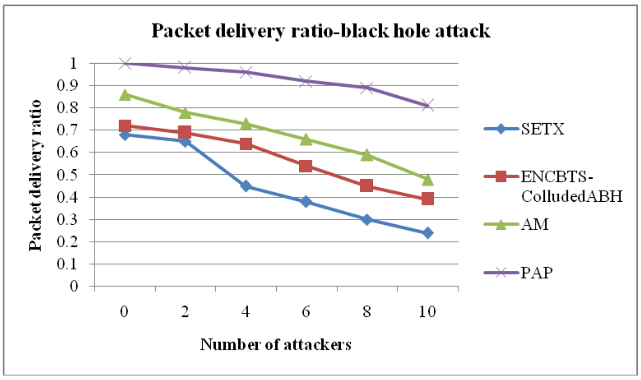

Figure 2. Comparison of packet delivery ratio with black hole attack.

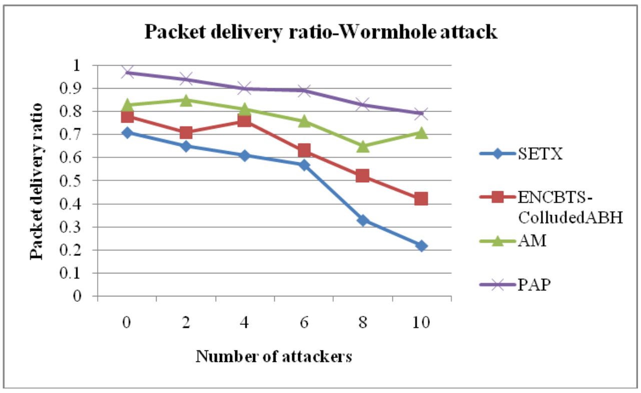

Figure 3. Comparison of packet delivery ratio with wormhole attack.

Figure 2 shows that the comparison of packet delivery ratio with black hole attack is calculated and compared by the various numbers of nodes. The sending request is reduced as the proposed protocol increases the packet size of request packets; it reduces the number of request packets more significantly which is shown in the Figure 2. Figure 3 shows that the packet delivery ratio in wormhole attack, the various protocols such as Secure Expected Transmission Count (SETX), ENCBTS-colluded ABH, Arthur-Merlin (AM) and Password Authentication Protocol (PAP) protocols, the proposed path assignment algorithm more accuracy than the other protocol which is shown in the Figure 3.

Detection rate

Detection rate is a difference between the number routing packets over received data packets and of routing packets that are generated during simulation time with the average data packet delivered from source to destination called detection rate ratio.

Detection rate ratio=(sum of ratio of routing packets over (Received data packets-Delivered data packets))/(The average data packet delivered from source to destination)

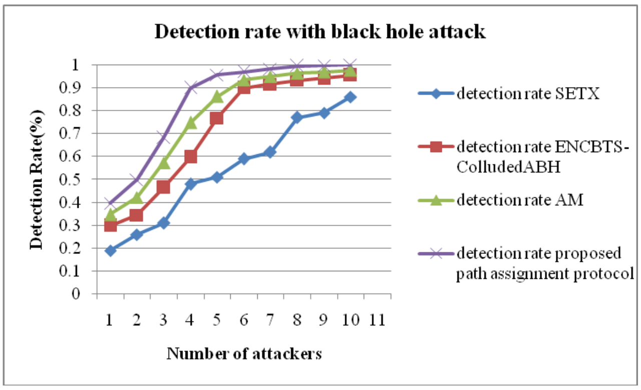

Figure 4. Comparison of detection rate with black hole attack.

The Figure 4 shows the graph of detection rate with black hole attack, and PAP protocol takes higher detection rate compare to the other protocol detection rate.

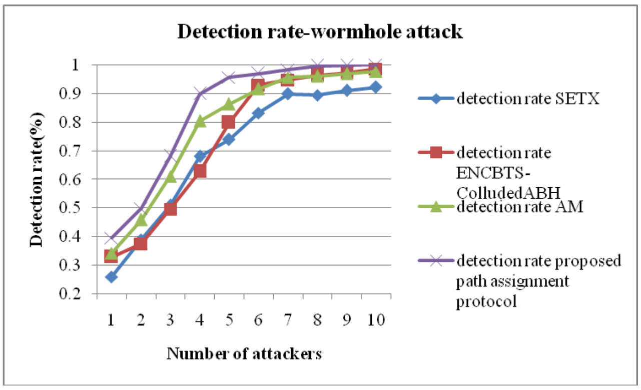

Figure 5. Comparison of detection rate with wormhole attack.

Proposed path assignment protocol evaluated with the help of various protocol such as SETX, ENCBTS-colluded ABH, AM and PAP protocols. The proposed PAP protocols give best performance for detection rate with wormhole attack. The

Figures 4 and 5 gives the detection rate comparison of existing technique with the proposed PAP protocols with irrespective malicious nodes. From this, it clearly shows that proposed technique achieves better detection rate than the existing protocols.

Data packet loss rate

Data packet loss rate defined with respect to the total number of nodes participation, the sending and receiving packet between the source and destination, the number of data packets sent by the sender and the number of data packets received by the receiver called data packet loss rate.

Data packet loss rate=(sum of sender and receiver packet count) × 100/sum of sender packet count

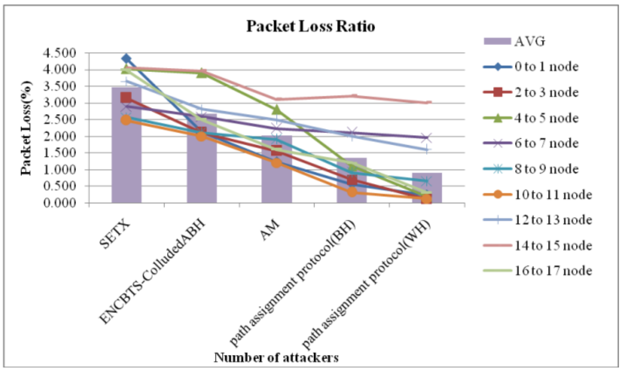

Figure 6. *Comparison of packet loss ratio with black hole and wormhole attacks.*

Figure 6 clearly stated that the packet loss ratio various algorithm. The proposed path assignment has 0.098% less loss than the existing system. The comparison of the packet loss is taken from the irrespective random number of reference nodes.

Discussion

To provide the security to the wireless sensor networks, the proactive and reactive attacks are main challenge of the security concern, to fulfil the this security concern, Our proposed system used to deduce and reduce the wormhole [7,17] and black hole [2] attacks by using the rapid response round trip time and the protocol based path assignment protocol. The attacks on the wireless sensor networks are caused the path between the route, path assignment protocol are managed the route discovery [5,18] and prevent the causes in the same path. Once the tunnel are appeared in between the node are again transmit the packet from the initial state [19]. This was used to make the path as secure and shortest path detection [10]. The proposed system consists of the following stages such as (i) Observe the transmission time between the malicious nodes by using Rapid Response Round Trip Time (R3T2). (ii) The Path Assignment Protocol (PAP) for finding the distance [8] between the suspicious nodes. (iii) Threshold based wormhole [9,20] and black hole detection [2] in WBSN. These three mechanisms are used to prevent the WBSN from the wormhole and black hole attacks.

Conclusion

Due to the attackers in the WBSN, the security is the one of the challenging issuing in data transmission, the rapid response round trip time mechanism and path assignment protocol are proposed to overcome the security challenging and detect the dangerous attacks like black hole and wormhole attack and also improve the security, packet delivery ratio, detection ratio and reduce the packet loss rate, of the mobile nodes, the new proposed algorithm of path assignment protocol and rapid response round trip time mechanism gives efficient and secure method for deducting the attacks like black hole and wormhole attack. In addition to that, nearest neighbour node selection used to discover the minimum short route, finally the transaction histories are stored to past transaction history route table. Each and every node communication history result will recorded for verify previous process. Once the transaction history is exists the packet did not send that route because of the route is already patterned or else the route has some malicious attacker. In the proposed scheme of our experiments make evident of the efficiency with the consideration of several performance metrics like packet delivery ratio, packet loss rate, detection rate ratio and so on.

References

1. Aziz O, Lo B, King R, Yang GZ, Darzi A. Pervasive body sensor network: An approach to monitoring the post-operative surgical patient. Int Workshop Wear Implant Body Sens Netw 2006; 1318.
2. Amiri R, Rafsanjani MK, Khosravi E, Amiri H. Black hole attacks in mobile ad hoc networks. J N Res Sci 2015; 9: 46-57.
3. Lalitha T, Uma Rani R. Challenges and surveys in key management and authentication scheme for wireless sensor networks in abstract of emerging trends in scientific research. Proc Emerg Trends Sci Res PAK Publ 2014; 740-751.
4. Tan SC, Kim K. Secure route discovery for preventing black hole attacks on AODV-based MANETs. Converg Int Conf 2013; 1027-1032.
5. Terence JS. Secure route discovery against wormhole attacks in sensor networks using mobile agents. Trendz Inform Sci Comp Int Conf 2011; 110-115.
6. Cai RJ, Joo CPH. A neighborhood connectivity-based trust scheme to identify active black hole attacks. Commun Sys IEEE Int Conf 2014; 543-548.
7. Maheshwari R, Gao J, Das SR. Detecting wormhole attacks in wireless networks using connectivity information. Infocam IEEE Int Conf Comp Commun 107-115.
8. Zhou Y, Lamont L, Li L. Wormhole attack detection based on distance verification and the use of hypothesis testing for wireless ad hoc networks. Milit Commun Conf IEEE 2009; 1-7.
9. Nait Abdesselam F, Bensaou B, Taleb T. Detecting and avoiding wormhole attacks in wireless ad hoc networks. Commun Magaz IEEE 2008; 46: 127-133.

10. Alem YF, Xuan ZC. Preventing black hole attack in mobile ad-hoc networks using anomaly detection. Fut Comp Commun Int Conf 2010; 3: 672.
11. Znaidi W, Minier M, Babau JP. Detecting wormhole attacks in wireless networks using local neighborhood information. Pers Indo Mob Rad Commun 2008.
12. Wang Y, Zhang Z, Wu J. A distributed approach for hidden wormhole detection with neighbourhood information. IEEE Netw Architect Stor Int Conf 2010; 63-72.
13. Athmani S, Boubiche DE, Bilami A. Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs. Comp Inform Technol W Cong 2013; 1-5.
14. Weerasinghe H, Fu H. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. Fut Gen commun Netw 2007; 2: 362-367.
15. Louazani A, Sekhri L, Kechar B. A time petri net model for wormhole attack detection in wireless sensor networks. Smart Commun Netw Technol Int Conf 2013; 1: 1-6.
16. Chauhan RK. An assessment based approach to detect black hole attack in MANET. Comput Commun Autom Int Conf 2015; 552-557.
17. Lu X, Dong D, Liao X. Worm planar: Topological planarization based wormhole detection in wireless networks. Par Proc Int Conf 2013; 498-503.
18. Jayanthiladevi K. Cluster based key management authentication in wireless bio sensor network. Int J Pharm Bio Sci 2016; 7: 89-94.
19. Wahane G, Kanthe AM, Simunic D. Detection of cooperative black hole attack using crosschecking with true link in MANET. Comput Intel Comp Res IEEE Int Conf 2014; 1-6.
20. Subha S, Sankar UG. Message authentication and wormhole detection mechanism in wireless sensor network. Intel Sys Cont Int Conf 2015; 1-4.

*Correspondence to

Manikandan KP

Department of Information Technology

Dhanalakshmi Srinivasan College of Engineering

India