International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2798-2808

Chronic Privacy Protection from Source to Sink in Sensor Network Routing

Mr. S. Sathees Babu
Associate Professor, Computer Science and Engineering
PSNA College of Engineering & Technology,
Dindigul, Tamilnadu, India.
E-mail: sbsdgl@gmail.com

Dr. K. Balasubadra
Professor and Head, Department of Information Technology
RMD College of Engineering and Technology
Chennai, Tamilnadu, India.
E-mail: balasubadra@yahoo.com

Abstract

In contemporary association, growths might be happen due to the Wireless Sensor Networks (WSN) which provided more flexible space for implementing and producing new initiatives. As well as the most important part placed in WSN is location privacy preservation. Though much effort put on source and receiver location security independently, there are no proper solutions discussed about location privacy from source to receiver. This paper considers end to end (E2E) location privacy which unfavorable to internal adversary in healthcare WSN. We introduce the new privacy preservation scheme that is more effective than previous four location privacy schemes that are Onward–conscious decision model (OCDM), Bi-Steering Model (BSM), Energetic Two-Way Interaction Model (ETWI) and Twisted Bi- Steering Model (TBSM). The new scheme called Hierarchy rift protection scheme which gives the effective E2E location privacy against internal adversary and also this scheme achieves the three major metrics for providing the privacy preservation hostile to internal eavesdroppers. This scheme uses hierarchy routing scheme for preserving source location privacy to create trap routes along the path to the sink from the real source. It attains privacy preservation and maximizes the network life time. This scheme systematically analyzes the energy consumption and monitors other factors that are chronic latency, transmission distance and time safety.

Keywords: Wireless Sensor Networks, End to End Location Privacy, Hierarchy rift protection scheme and internal attackers.

INTRODUCTION

Wireless sensor networks built-up the low cost wireless communication systems and sensor devices. WSN developed promptly under the domains such as infrastructure domain, Military applications, healthcare application and Habitat monitoring, etc. WSN advances their field into healthcare systems. Sensor technology has raided medical devices to restore wired devices in hospitals and related fields. Alongside, more people are breathing with chronic diseases such as heart disease, cancer, Alzheimer's, and other forms of dementia, placing larger burdens on healthcare systems [1]. The healthcare system issues are privacy breach, compromise the healthcare services and disabling patients to avail healthcare facilities.

In Fig.1. Sensors data of these healthcare applications in WSN composed by information about the health status of the patient and stored in a database. Heart rate, Blood Pressure, distance traveled through walking and running, room temperature and etc. are commonly said as the information about health status. The healthcare applications have the security threats such as eavesdropping or snooping, routing attacks, masquerading, privacy, data reply and denial-of-service attacks. Its security requirements are Data confidentiality, data integrity, data availability, data authentication and user's consent. Data encryption and decryption, secure authentication, secure routing and Law and regulation for users are few security mechanisms used in healthcare system to overcome from the security threats.

Some of the local threats or internal adversary is concerned in wireless sensor networks [2]. The threats of WSN distracting the common functionalities as well as it are very easy to collapse the whole network. It is easy to capture the location of source node with the help of eavesdropping. When the node compromised internally by malicious nodes, it injects false information into the network. This is major issue in healthcare system [3]. Because of this issue, anyone's medical data can be disclosed to unwanted personals, the original data may be altered and sent to the doctors, and modified data contains wrong medicine information, etc. so that the healthcare system could do with end to end location privacy in WSNs. The source sends the sensed and aggregated data to the sink through several wireless hops. There is data administrator, doctor and caregivers listens continuously about patients' data and particularly about critical patients. The health advisor or doctor gets analysis of critical patient and care should be taken I the location itself. The analysis process on location privacy is exceptionally complicated due to internally compromised nodes. The compromised node can certainly track the path from source to sink and crumple the data or tailor the data. Due to these reasons, location privacy is one of the most challenging security components in wireless sensor networks.

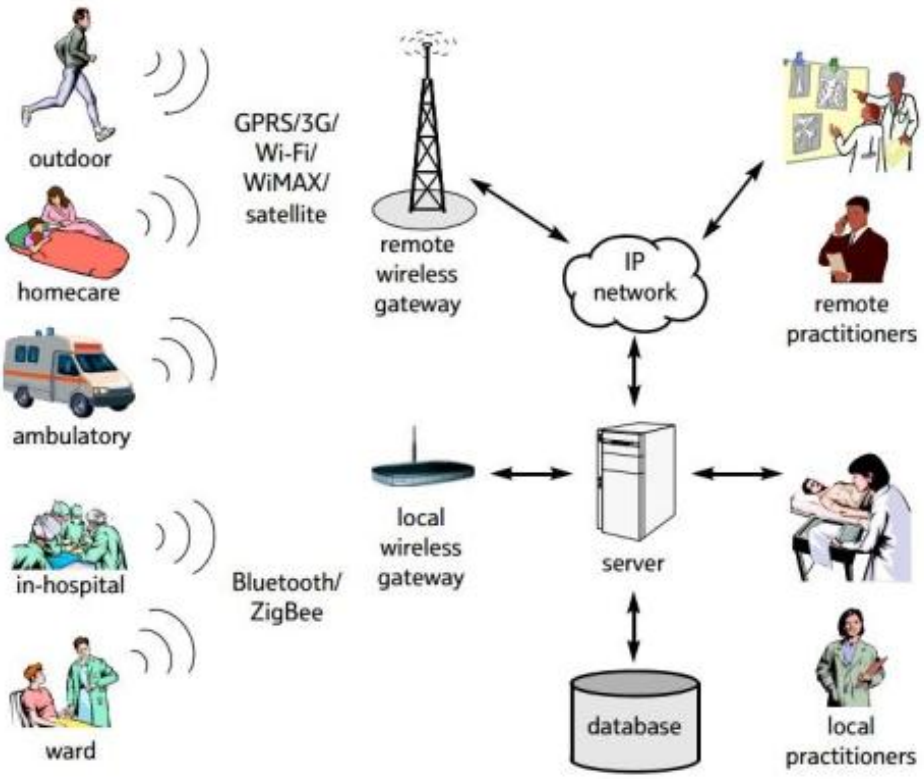

Figure 1. Healthcare Monitoring System

As mentioned in earlier works, we have either source location privacy or sink location privacy [4]. There is no apposite scheme available to preserve the privacy from end to end location. The previous works described various end-to-end location privacy preservation methods for transmitting messages from source to sink. These projected four methods can preserve against the internal adversary. The four end to end privacy schemes are (1) Onward–conscious decision model (OCDM), (2) Bi-Steering Model (BSM), (3) Energetic Two-Way Interaction Model (ETWI) and (4) Twisted Bi-Steering Model (TBSM). Time safety is one of the metric to monitor the performance from the initial state on the eavesdropper. When the eavesdropper is point out the source or destination, it finds the tracing rules and ends at the moment. Chronic Latency is one other metric used to find the average time take from source to sink. The other metric used to measure the average number of packets transfer in the network within stipulated time.

In Onward–conscious decision model (OCDM), every node transmits a incoming packet to a randomly selected node from its neighbors whose hop count to the sink is not larger than its own. The Bi-Steering Model (BSM) is working with tree topology which can enhance the location ambiguity. In this model, original messages are sent the length of the shortest path and provide a space for the eavesdropper to guess the location of the source or sink. In Energetic Two-Way Interaction Model (ETWI), tree branches are created dynamically to increase the performance continuously. An alternative source and sink are adopted in Twisted Bi-Steering Model (TBSM) to crack the potential threat, which protects the contender from cracking the location of the source and sink [4][5].

In this paper, we propose Hierarchy Rift Protection Scheme (HRPS) for preserving location privacy from source to sink. This scheme provides effective end to end location privacy against local eavesdroppers or internally compromised nodes. HRPS is unusual from modern research in which it creates more diversionary routes than the traditional routing schemes. This scheme greatly improves E2E location privacy and the lifetime of the network. The purpose the HRPS scheme to analyze the corollary of concurrently protecting the location privacy of the source and destination. The previous four schemes for E2E location privacy have divergent performance results on protecting the source and sink location privacy. HRPS is more effective and achieves strong privacy preservation than the previous four schemes. This privacy preservation includes defense against the track-inclined attacks.

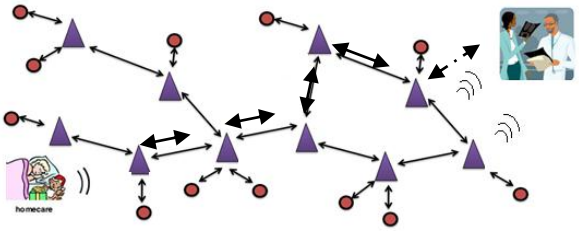

Figure 2. Route Planning

In Fig.2., the network model explains how the patients' data can be directed via many wireless hops. The direction path from source to destination monitored continuously. This kind of support used to identify the eavesdroppers in this model. The secured direction path shows in the figure using arrows. The dashed arrow mentioned as wireless communication path. The system architecture designed as shown in Fig.3.

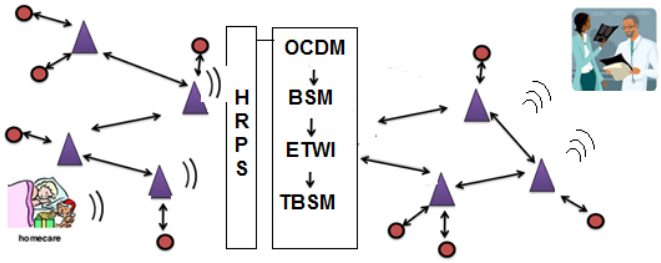

Figure 3. System Architecture

The sensed patient data transmits through the wireless points i.e., sink. The source node first sends the data to the phantom node which is located away from it in phantom routing. The source node's data cannot send directly to the sink. The phantom node operates as a trap relaying the data in a shortest path to the sink [6]. As a result of the fact that presently accessible phantom routing scheme always has the phantom node routed to the sink directly; it allows the compromised node to trace back along the route to phantom nodes. An upfront solution is to have several diversionary routes to the sink. It is difficult for the compromised node to determine which route the actual data is in. Although an enhancement in source location privacy, the energy consumption is more and the network life time is reduced in phantom routing. HRPS create more diversionary routes than the traditional phantom routing schemes, which seriously enhances the source location privacy and at the same time the network life time does not decline.

RELATED WORK

The location privacy threats can exist in context-based privacy threats of wireless sensor networks. One important aspect of context based privacy in several applications is source location privacy. The attacker's ability can be expected from globally and internally. There are several algorithms, protocols and models available for handling global attackers and few extensive researches are going against compromised nodes or internally malicious nodes. Location privacy preservation in wireless sensor networks can be performed independently in both ends such as source and destination [6][7][9].

P. Kamat, Y. Zhang, W. Trappe & C. Ozturk. [6] presented a new method for source location privacy preservation, which related to the "Panda-Hunter'' problem as an application for monitoring based sensor networks. In their view of the description, the location privacy is crucial. The Phantom routing protocol utilizes a random walk technique to prevent attackers from identifying the source. Y. Xi, L. Schwiebert, W. Shi. [7], projected a two-way random walk routing protocol called greedy random walk. This protocol can be employed from both the source and sink. It can diminish the chance for an eavesdropper to collect the location information. W. wang, L. Chen., J. Wang. [8], defends the source location privacy by using inclination angles to ensure that every random walk gets away from the region close to the source. In this paper, they proposed a scheme to improve the source location privacy. G. Chen, Y. Ouyang, Z. Le, J. Ford, F. Makedon, [9], developed method that is created loops in the network. The adversary mentioned by these authors has to move in the region of these loops, which are directed from the real path. This procedure guarantees a high privacy according to the discussion made by the authors. This routing scheme delivering message flows to diverse disjoint routes. This scheme formulated the performance bound for any routing scheme. Li and Ren [10, 11] protected the source location privacy in the course of a two-phase routing process. In phase one, the packet passes through randomly through the intermediate nodes before it is routed to a ring node. In second phase, it causes and the original data packet is mixed with other packets via a network mixing ring (NMR).

Deng et al., recommended the privacy preservation of the base station against the traffic-rate analysis attack [13]. This scheme operated by randomly delaying the transmission time of each packet. The authors also planned to give protection against the traffic analysis attacks. First, they measured a multi-path routing for granting intrusion tolerance against separation of a base station. This paper also suggested anti-traffic analysis strategies to cover the location privacy of the base station. Y. Jian, S. Chen, Z. Zhang, L. Zhang, [14] proposed the receiver location privacy against the packet tracing attacks. The directions of both incoming and outgoing from a sensor node are dependably detached. False messages are also introduced to get a longer safety period with the cost of increasing the energy consumption. G. Chai, M. Xu, W. Xu, Z. Lin, [15] and [12], presented the sink location privacy safety model against the external adversaries. The planned model of this paper can attain k-anonymity in the network, so that at least k entities are indistinguishable to the nodes around the sink.

Four location privacy protection schemes [4] are proposed and discussed for ensuring the end to end location privacy. They are known as Forward Random Walk, Bidirectional Tree, Dynamic Bidirectional Tree and Zigzag Bidirectional Tree respectively. The DBT scheme and ZBT scheme build some branch routes in the route from the original source node to sink node to improve the privacy protection performance. In the DBT scheme, real messages are delivered along the shortest path, making it possible for the eavesdropper to infer the location of the source or sink by extending the line of the shortest path. So, a proxy source and a proxy sink are adopted in the ZBT scheme, which prevents the adversary from inferring the location of the source or sink easily.

The drawback of the said four methods is that none of them considers the location privacy from the source to sink. The location privacy of the source and destination has been discussed independently in [17, 18]. In [17], it is proposed the information leakage-aware cloaking (ILC) to defend the location privacy of the users. The flow is to cloak the

anonymous set by using multiple anonymous spatial regions, each of which contains more than m users. In [18], it is proposed that the several advanced PIR-based methods to guarantee no information leakage by using the same query plan for all queries. It is also proposed to achieve an identical chronological order of the page retrievals and adding fake pages into the query procedure. Therefore, the adversary cannot distinguish any queries. However, these schemes focus on the privacy protection which is usually a database-driven system and is not suitable for the WSNs.

LOCATION PRIVACY PRESERVATION SCHEMES

The Location Privacy Preservation is one of the most recent researches in wireless sensor networks. The existing researches on this field shows only either side of privacy that is source location privacy or destination or sink location privacy. Only few researches demonstrated the location privacy on both sides with substantial drawbacks. No one can examine the end to end location privacy preservation from source to sink concurrently against internally compromised node or an adversary in WSNs.

The previous E2E privacy schemes [4] are Onward–conscious decision model (OCDM), Bi-Steering Model (BSM), Energetic Two-Way Interaction Model (ETWI) and Twisted Bi- Steering Model (TBSM). Also, these schemes are monitoring the time safety which begins from the initial state on the adversary, finding the tracing rules and ends at the moment when the adversary is point out the source or destination. The second metric is focusing on E2E latency which shows the average time take from source to destination and the last metrics is defined the measured the average number of packets transfer in the network within time. In Onward–conscious decision model (OCDM), the monitoring data communicate from source to destination in a standard or fixed path means then, it will be very easy to know the location of the animal and also hack the original information about the location of the animal. For this problem we are providing the solution to achieve the E2E location privacy by making the communication in a random path of nearby node selection up to the destination controller.

The initial state the source node will check whether the hop count is empty or not. If the Next_hop is empty then it can create the onward random list which contains three major list that are smaller list, equal list and next list. While next hop is getting real data then the source node will select the next node from ORLi at the next hop. Finally the real data will take one step onwards to the destination controller. Here the main drawback is the safety time becomes high, because of large process and this model is not very much hard to hack by the internal adversary.

To overcome the drawback of first scheme the second scheme is introduced, called the Bi-Steering Model (BSM). In that, BSM will used to create the sub branches at source and destination side and those branches are hiding in the structure of tree topology. When the data transfer from one source node into destination node, the sub branches are used to collapse against the local attacker. This type of structure is used to provide high difficulty for adversary to find out the original data in N/w flow. For that, we are creating and setup the tree structure in BSM scheme for providing the E2E location privacy. The goal of BSM is, the original data can transmitted from source to destination within the minimize path. For that, the dummy data are release from sub branch nodes. When the original data transfer from real path on source to destination means then the local attacker is involved to trace backward on the source side as well as sink side because of try to capture the original data path to collapse the data.

The initial stage of the hop count and child branches must be empty. Then we can create the nearby node set NNi and the smaller list SLi based upon the list we can randomly select a node from CLi as Next_hop. The child node will be chosen from dynamic selection by using the command of NNi − Next_hop. When the destination node can get the original data it will onward selection the data to next_ hop. Then its check the condition If Hk > (1 − α/ 2) Hs which means create the branches will the help of Hk > (1 − α/ 2). Here we are using TsL (tree set length) with the help of TsL we can send the branch request and monitoring the length of the branches from source to destination. If the condition Hk < α/ 2 Hs is satisfied then the dummy data are travel from the real path. Otherwise the original data will be travel from real path.

The purpose of Energetic Two-Way Interaction Model (ETWI) is to transfer the original data within the time which can increase the tracing time to be difficult for the attackers. In this model the source node dynamically passing the data to the destination node by using random selection on the neighbor in the model of onward selection list. Here we implement the dummy nodes as branches in both source side as well as destination sides. In previous model the dummy branches are created but in this model the dummy nodes are deployed at both side and the fake data will be back onward to the original node path to deviate the adversary. In this type of tree structure if the attacker is present in flow of transmission path, then the dummy nodes sends the dummy data and it will be combined to the original data such as, the adversary cannot find the correct data during the data transmission time. At the same time if the sink controller gets the dummy data message means then the dummy sub branches nodes are act as the relay to reselect the another sub branches node. Here the main disadvantage is, we deploy the dummy nodes for sending the dummy data to the original path such as the E2E latency is become very high as well as energy lifetime will become very low.

The initial state of this model defined as empty and sub branches are must be an empty then we can able to create onwards list. When we getting the original data from the node N then the dynamic select a node from Next_hop and forward the data to Next_hop which is Child_node ←Dynamic Select (NNi − Next_hop).if the hop count of the source node is less than to both source and sink nearby nodes means, then it will be set the tree set list for branch request and length. And it will be onward randomly choose the node to passing the data for the destination. Otherwise the nearby nodes are smaller than hop source at the same time current nearby node which is less than to another neighbor node. If the second condition is satisfied means then the dummy message will be combined to the original node with the help of tree set length.

Twisted Bi- Steering Model (TBSM) introduce the proxy's for both source side as well as sink side and also created the branches node for passing the dummy message. In this model three important part will be placed as important role that are from the source node to the proxy source, the second step is from the proxy source to the alternative sink and the final step is from the alternative sink to the sink controller. Here we deploy the proxy source and sinks for both sides such as, the source node send the data in the shortest path to sink controller. In the first step the data will move over to proxy source. When the proxy source gets the data, then it will check whether the data is correct data or dummy node.

The main problem is those proxy source and proxy sink are highly expensive. Also, the energy of the tree structure is become more critical to save the life of the networks. Finally, we can compare those all four existing schemes and its providing the different performance results for each stages. For that we are plan to introduce the new scheme is called Tree Diversion Protection.

PROPOSED HRPS SCHEME

In this paper, we propose Hierarchy Rift Protection Scheme (HRPS) for preserving location privacy from source to sink. This scheme provides effective end to end location privacy against local eavesdroppers or internally compromised nodes. HRPS is unusual from modern research in which it creates more diversionary routes than the traditional routing schemes. This scheme greatly improves E2E location privacy and the lifetime of the network. The purpose the HRPS scheme to analyze the corollary of concurrently protecting the location privacy of the source and destination. The previous four schemes for E2E location privacy have divergent performance results on protecting the source and sink location privacy. HRPS is more effective and achieves strong privacy preservation than the previous four schemes. This privacy preservation includes defense against the track-inclined attacks.

Antagonist model

It is presumed that the malicious nodes are equipped with highly furnished than the other nodes in this example scenario. Malicious can be either locally malicious or globally malicious. Local malicious nodes or internally compromised nodes are supposed to scrutiny the network traffic locally which eavesdrop the packets within the transmission range. Globally malicious nodes [12] attain a wide range of network traffic which can eavesdrop on each transmitted packet in the network. In this proposed model, we concentrate on the location privacy protection from source to destination i.e., sink against the local malicious nodes. The following characteristics of a local adversary illustrated from the healthcare application.

The malicious nodes are able to have sufficient energy resources, enough computation capability and plenty of memory for data storage. They can recognize the location of instant sender based on its high capacity and can move to the sender's location immediately. The malicious node randomly opts whether to map out the source or sink when it captures the transmitted packet. The malicious node can confine the source of a traffic flow and tracing back hop by hop. If the distance of the destination is too short, then malicious node can detect the destination exactly. The malicious node won't mutate packets in transmission, amend the routing path or spoil sensor devices. In spite of this, the malicious node may accomplish passive attacks like eavesdropping.

Overview of the HRP Scheme

The Hierarchy Rift Protection Scheme (HRPS) is one of the most security effective schemes and provides the end to end location protection against local eavesdropper. Also, this scheme maximizes the network lifetime. In this scheme, the routing hierarchies are established unvaryingly and the malicious node cannot assume the source location derived from the nature of the hierarchy. As per the principles of the scheme, the energy consumption of the node in junctures is not amplified and network life time is not declined. If the sink or destination is away from the current region, the scheme creates more incidental routes for protecting phantom node. HRPS has put into practice by two different phases. In the first phase, it establishes the backbone route path direct to the network edge which founded on the presented phantom routes. Second, it establishes redundant routes as many as possible in that zone. Fig.4. shows the illustration of the HRPS routing which seeks the protection of source and sink respectively. The outline of this scheme is to establish the phantom node away from the source node and then establish the routing path in the direction of the sink. It creates hierarchy routes from all other nodes and the end nodes are known as fake nodes.

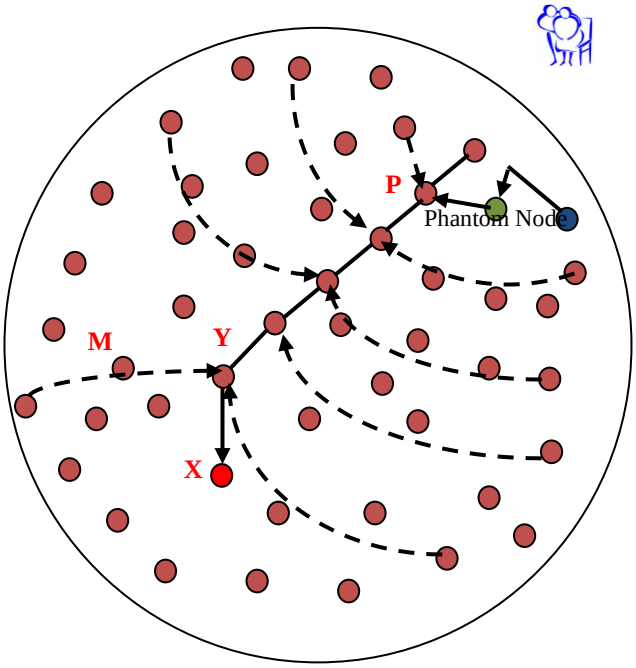

Figure 4. HRPS routing exemplify

HRPS Algorithm

HRPS routing network formation and process is classified into three phases which are going to integrate these phases into one scheme for providing secure end to end location privacy protection in healthcare monitoring systems. The three phases are,

1. Hierarchy Route Network Formation,
2. Hierarchy Routing
3. Wipe out the Hierarchy Routing

The creation of a phantom node is based on the previous methods from [19, 20]. The prerequisite of electing the phantom node is that it is as much as away from the source node.

Hierarchy Route Network Formation

First, the algorithm established the limb of the hierarchy route formation with phantom node. Also, this route establishes its track and supported sub branches. The node which is appointed as a phantom node has not involved in backbone track usually because the node can be easily recognized by the malicious nodes or attackers. So, the present implementation can be very difficult to find the original data and the real data of the phantom node which is positioned in any side of tracks. The travel of this node process can be both directions like down-left direction to the node Y and top-right direction to other nodes. In figure-4, it shows the backbone route path set as X – Y to P. The phantom node selects a nearby node which is contiguous to the destination or the backbone route. Here, it selects P node which is nearby backbone route node from the phantom node. This is continuously passed through to node P which is known as Intermediate node. Then, it starts to ask the counterfeit information or packets from top-right direction. The process of receiving replica packets from nearby nodes can be performed at fixed time intervals.

Second, it is establishing the backbone route path from the intermediate node P. The packets are transmitted from intermediate node to sink through the nodes Y, X. This transmission performs using the traditional shortest path routing algorithm. Based on shortest routing, the node P intermediate node selects the node nearby the sink for its transmission. Until the packet reaches the sink, the shortest route continues. If the intermediate node takes another direction to transmit the packets, it finds the different branches based on the fake messages. Until it reaches the network border region, the request packet transmission continues through the neighbor nodes. Third, there are establishing a split route from the backbone route when the node Y in backbone path. The node Y sends the request for replica packets to split routes till it reaches the end of the network region.

Algorithm-1: Hierarchy Route creation

INPUT: X, Y, P, Pn, h

OUTPUT: path created for transmission

Establish a phantom node based on the reference article [6]

Ra = Random(0,l)

If Ra >= ½ + 1/h then

Dp ="right"

Else Dp =”left”

Rq= (ID_{Pn}, type, b_n, locality, L_c , Dp, pad)

RevRq = K_{Pn}^{x}(ID_{Pn}, type, b_n, locality, L_c , Dp, pad)

Nearby_node = Pn

while (Nearby_node (RevRq).b_n > 0)

Exchange the value of the Nearby_node as the next hop

Nearby_node = GetNextOnLeastHop(R_L, Dp);

Nearby_node = GetNextOnEqualPath (R_L, Dp);

$b_n = b_n - 1$

P = Nearby_node

Nearby_node=Pn

while (Nearby_node != L_c)

Exchange the value of the Nearby_node as the next hop

Nearby_node = GetNextOnMaxHop(R_L, Dp);

Nearby_node = GetNextOnEqualPath (R_L, Dp);

for node P is TRUE

while (GetNodeOnMinHop(P) != S)

P = GetNextOnMinHop(P)

while (GetNodeOnMaxHop(P) != L_c)

P = GetNextOnMaxHop(P)

for node M in (P → Y → X)

If (M.hop == locality)

Nearby_node = M

while (Nearby_node != L_c)

Exchange the value of the Nearby_node as the next hop

Nearby_node = GetNextOnMaxHop(R_L, Dp);

Nearby_node = GetNextOnEqualPath (R_L, Dp);

Hierarchy Route Creation Algorithm have various inputs like phantom node Pn, Intermediate node P, nodes X, Y and M,

height of the route path, message from current location node, L_c, Direction point, Dp, branch hop number, b_n, current position of the node, R_L, and Sink, S. It takes several steps to identify the path nearer to the sink and formulate a path structure from phantom node. Finally, it produces a routing path in this hierarchy approach.

Hierarchy Routing

In hierarchy routing, it verifies whether all route nodes are concerned by various rift routes configured in previous phase of algorithm. Routing of packets happened with either original data packet received by the node or fake message packets generated by the node in a fixed time. Once the original data packet received by the node, it transmits the data packet to the other nodes. Otherwise, the fake messages can be created by node itself at a fixed time and equipped to transfer the replica packets. Once the sink controller gets the original data the current transmission process come to end. After that the sink controller responses to nodes through a message 'data received' till nodes are in network border. Performing the hierarchy routing protection are made by data transmission from phantom node to destination node and sink to source nodes.

Algorithm-2: Hierarchy Routing

INPUT: L_c, N

OUTPUT: packet transmitted at fixed time (routing)

For each node N on the hierarchy route

When the fixed time the message comes,

If N receives the original data packet

Send the original data packet to GetNextOnMinHop(N);

else

Send replica packets (fake messages) to GetNextOnMinHop(N);

Wipe out the Hierarchy Routing

In this phase of HRPS, the termination of present route related to the phantom node and intermediate data node. Until, both the intermediate node and the phantom node have not received the original data packet within the fixed time period, the present hierarchy route path will be discarded. The caregivers supervise the size of the data packet and also determine the transmission time at a fixed period. If the sink node acquires the wrong data packets or fake messages continuously, then the routing stops to transmit the messages in the same routing path. Once all routing branches are getting the stop information, then it will discard itself for deviate the adversary.

Algorithm-3: Trash the Hierarchy Route

If a node acquires a "stop" information

Send current data packet to all nearby nodes

Bring to an end from transferring any other data packets

The benefit of HRPS algorithm provides more effectiveness for achieving the end to end location privacy protection against internal eavesdroppers. Also, the energy of the routing network is little high, it won't influence the lifetime of the network. This algorithm is very efficient because of the rift routes are active only when the phantom node is present in nearby routing network border. Other benefit of this scheme is to share energy from source node's energy whenever its nearby nodes are got emergency alert.

PERFORMANCE INVESTIGATIONS

Security in healthcare applications is vital and promising research focus in the current world. The patient or user data share on the wireless communication in WSN of healthcare applications. Given that the wireless communication ranges are not restricted, the compromised inside attacks even cause more significant risks to the user or patient. For example the routing sensitive data into wireless communication network cause either the data can be hacked or malfunctioned. So, the researchers must consider robust security and privacy needs where the people life in at high risk. The researchers also think about end to end privacy preservation, energy consumption during the nodes at backbone route path and end-to-end Latency between the sensor and data server.

Simulation Environment

Simulations are accomplished using Network Simulator with highly developed sensor patches. We perform and analyze our algorithm based the metrics like energy efficiency, estimated or delay time, E2E privacy, computation and communication cost. The simulation parameters are primarily organized as follows: Let us assume a heterogeneous sensor network with 200 numbers of sensor nodes are randomly distributed in the 4000 * 2400 m^2 as network field size with respect to the healthcare applications. The base station is located at one point in the field. Nodes will have 250m as the transmission range and 550m as their sensing range. The typical number of nearby nodes for a node is 6.17. The initial battery set as 1 x 10^6 J for each node in the network. The interference queue length is chosen as 50 packets in each node. We take the packet size as 1024 bytes at a packet rate of 8 packets per second. The minimum speed is taken as 5 ms whereas the maximum speed is 8ms.

Security and Privacy Discussion

At the outset, this paper investigates the security concerns in healthcare applications of wireless sensor networks based on the previous four methods discussed in section-3. These four

schemes concern to end-to-end location privacy protection which were launched to protect both the ends against local eavesdropper. This progression might insist on the location privacy of a source to destination or sink, i.e., the end-to end location privacy is facilitated. The word eavesdropper is used for the person in healthcare application who is malicious internally or the internal nodes compromised by malicious nodes.

In the Onward–conscious decision model scheme, each node transmits a received packet to a node randomly selected from its forward neighbors whose hop count to the sink is not larger than its own. The problem with Onward–conscious decision model is as follows: The OCDM model preserves the end to end location privacy by randomizing the transfer route. The issues are, it will raise the end-to-end latency, the level of energy consumption is high and it also takes much transmission time. Because of fixed path the nodes, the original data packets can send in short time. However, the transmission is increased when the model increase in number of nodes. Another flaw of this scheme is that the node has only conscious about its neighbors, but not the other nodes. As a result this flaw, the security level is not high in this scheme. The way to improve it is to add dummy message in the network.

In the Bi-Steering Model, a tree organization is employed at two ends of the transmission route to enhance the location privacy from the source to sink. The problem with Bi-Steering Model is as follows: though this model protects both the ends by creating the branches on both ends, there are many chances that the eavesdropper may apply some smarter scheme and can trace the route. While using this model, it is possible to divert the eavesdropper from its regular route, but the smart eavesdropper may find out the location at the ease. So, the eavesdropper is able to locate the route by moving simply from source to sink or sink to source instead of using branch paths in the network.

In the Energetic Two-Way Interaction Model, the trees branches created dynamically to make better in the performance. The problem with Energetic Two-Way Interaction Model as follows: this model prevents the network region along with routes from its improper working. Because of the original messages and the fake messages are travelled into the network nodes now and again, it may cause into traffic congestion and the multiplied delivery time. Another flaw of this model is that the nodes have to remain active in all time because these nodes have to receive packets periodically.

In Twisted Bi- Steering Model, two proxy servers are added to divert the eavesdropper which act as source and sink. These proxy source and sink will act like original source and sink. The problem with Twisted Bi- Steering Model is as follows: but the alternative sink is nearer to the source, the twisted routing will be invalid. It is also required that the proxy source ought to away from the sink. In case of any failures in these approaches, this model won't work properly. Due to the problem associated with the calculation of distance between source and proxy sink, the eavesdropper cannot perceive the literal location of original source. Another flaw of this model is that it consumes a lot of energy because of more nodes, proxy source and proxy sink being there in the network.

To conclude the discussion, it takes part of the discussion about the proposed Hierarchy Rift Protection Scheme (HRPS). In this scheme, it creates more rift routes for original data packet transmission and provides constant network life time even if the nodes consumed additional energy. A little modified phantom routing used in this scheme for achieving end to end location privacy. Finding backbone route is very tedious process for the eavesdroppers because of its rift routes and phantom node. So, this scheme automatically enforces the needed security along with end to end location privacy.

Table 1. Investigation report on security and privacy

Privacy Preservation Routing Schemes	Source Location Privacy	Receiver Location Privacy	End to End Location Privacy
OCDM	YES	NO	NO
BSM	YES	NO	NO
ETWI	NO	YES	NO
TBSM	NO	YES	YES
HRPS	YES	YES	YES

End Result Investigations

The result investigations of these five schemes are under end to end location privacy schemes. The OCDM scheme attains the huge presentation while the shortest path scheme has the lowest safety period.

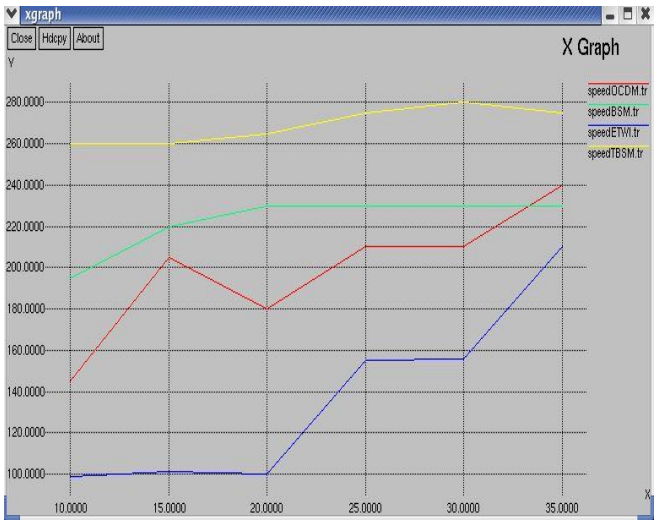

Figure 5. Safety period of Location privacy preservation schemes

The source location confines by the eavesdropper at the ease than sink location. Fig.5. describes the safety period of the sink location privacy is also superior to the source location privacy. The safety period of all schemes multiplies with the

raise of hop count. Fig.6. reports the investigations of these five schemes based on end to end latency. The original message packets are delivered from source location to the destination location with the help of BSM scheme and shortest path scheme. This process would achieve the shortest end to end latency. The end to end latency of TBSM is the leading value as it utilizes the twisted and dynamic routes to mislead the eavesdropper. When the hop count increases, the end to end latency of OCDM and ETWI schemes surpasses that of the TBSM scheme.

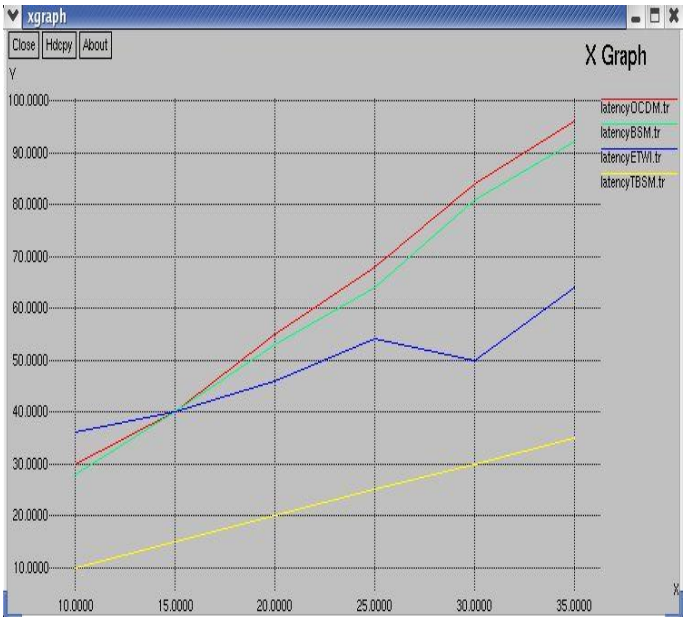

Figure 6. End to end latency of Location privacy preservation schemes

Fig.7. depicts based on energy consumption of these five schemes. The shortest path scheme spends the minimum energy since it does not create any fake message packets and the original message packets are delivered along the shortest path.

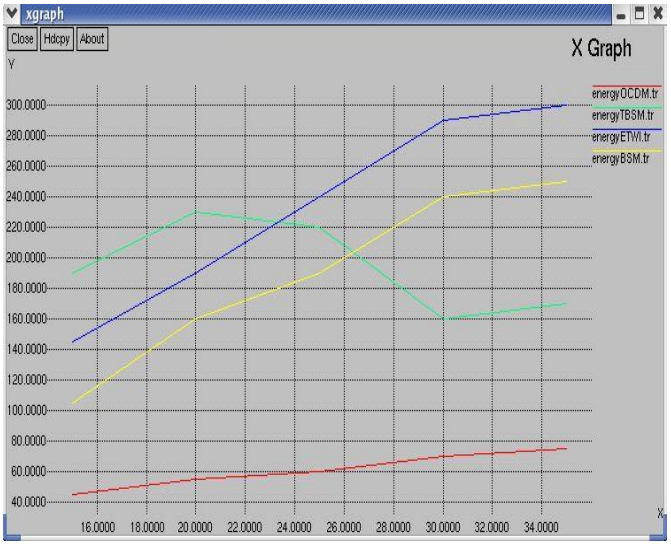

Figure 7. Energy Consumption of Location privacy preservation schemes

The OCDM scheme consumes second least energy due to the reason that it does not create any fake message packets. When the hop count is less than 20, the TBSM scheme spends a large amount of energy because the additional sink would be selected and extra fake message packets are created than other schemes. When the hop count is larger than 20, the energy consumption of the ETWI scheme is major, because more branch routes are engaged than other schemes. The metrics time safety, E2E latency and energy lifetime will be used to analysis HRPS scheme and triggered the E2E privacy preservation. First, Time Safety begins from the initial state on the compromised node, discovering the tracing rules and ends at the moment when the compromised node indicates the source or destination. Second, E2E latency shows the average time taken for a packet to make a journey from source to destination. Third, Energy Lifetime examines the packet transmission and simply defined as the energy lifetime measured by the average number of packets transfer in the network within time.

Table 2. Illustration of performance metrics of privacy preservation schemes

Privacy Preservation Schemes	Hop Count (<20)			Hop Count (>20)		
	Safety Period	End to end latency	Energy Consumption	Safety Period	End to end latency	Energy Consumption
OCDM	Low	Modest	Low	High	High	Low
BSM	Modest	Modest	Modest	Modest	Modest	Modest
ETWI	Modest	Modest	Modest	High	High	High
TBSM	High	High	High	Modest	Modest	Modest
HRPS	Low	Low	Modest	Low	Low	Modest

Table 1. and Table 2. exhibits the security and result investigations of the privacy preservation schemes respectively. From the above results, it concludes that our proposed system provides end to end location privacy from the source location to the destination location properly. The other schemes are satisfied with either source location privacy or receiver location privacy independently except the TBSM scheme. Though, the TBSM scheme provides both end privacy preservation, the few properties are not satisfied in the specified threshold. However, The HRPS system has the modest energy consumption,

CONCLUSION

The end to end location privacy is seemly further significant concern in healthcare applications of wireless sensor networks. In this paper, it is proposed five privacy preservation schemes for protecting the location privacy from source to the destination concurrently against internal attackers or local eavesdropper while transmitting message packets between them. HRPS scheme has many advantages over the previous phantom routing protocol. In previous research, there is only one path in phantom route and creating a phantom node is away from the source node. HRPS can avoid this issue by generating a hierarchy backbone route and many rift routes. This approach enhances the security without affecting network lifetime. The extensive result investigation report deal with hierarchy route scheme is better than presented privacy preservation schemes. The proposed scheme has high network life time. Although, the total energy consumption of this scheme is a little more than other schemes, it maximally reduces the energy consumption in hotspot.

The discussed privacy preservation schemes have different performance on protecting the source location privacy and destination location privacy. This work is going to substitute in the work of obtaining network level privacy in wireless sensor networks as an extension of privacy preservation. This extension of proposed work might be treated as my future work.

REFERENCES

[1] Vivek Agarwal, Security and Privacy issues in wireless sensor networks for healthcare, in: Proc. of the Springer Conference on HealthyIoT, 2014.

[2] Dr. Afsanesh Minaie, Dr. Ali Sanati-Mehrizy, Paymon Sanati-Mehrizy and Dr. Reza Sanati-Mehrizy, Application of Wireless Sensor Networks in Healthcare System, ATLANTA, 120th ASEE Annual Conference and Exposition, 2013.

[3] Wassnaa AL-mawee, Privacy and Security Issues in IoT healthcare applications for

the Disabled users a survey, Master's Theses, 651, 2012.

[4] H. Chen and W. Lou, On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks, *Pervasive and Mobile Computing, http://dx.doi.org/10.1016/j.pmcj.2014.01.006, 2014.*

[5] Jun Long, Mainxiong Dong, Kaoru Ota, and Anfeng Liu, Achieving Source Location Privacy and Network Lifetime Maximization through Tree-based Diversionary Routing in Wireless Sensor Networks, IEEE Access, open solutions, volume 2, pp:633-651, 2014.

[6] P. Kamat, Y. Zhang, W. Trappe & C. Ozturk, Enhancing source-location privacy in sensor network routing, in: Proc. of IEEE ICDCS, 2005, pp. 599–608.

[7] Y. Xi, L. Schwiebert, W. Shi, Preserving source location privacy in monitoring-based wireless sensor networks, in: Proc. of 2nd International Workshop on Security in Systems and Networks, SSN, in Conjunction with IPDPS, 2006.

[8] W. wang, L. Chen., J. Wang., A source-Location Privacy Protocol in WSN based on Locational angle, in: Proc. of IEEE ICC, pp: 1630-1634, 2008.

[9] Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon, Entrapping adversaries for source protection in sensor networks, in: Proc. of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM, pp. 25–34, 2006.

[10] Y. Li & J. Ren, Preserving source-location privacy in wireless sensor networks, in: Proc. of IEEE SECON, 2009.

[11] Y. Li, J. Ren, Source-location privacy through dynamic routing in wireless sensor networks, in: Proc. of IEEE INFOCOM, 2010.

[12] K. Mehta, D. Liu M. Wright, Location privacy in sensor networks against a global eavesdropper, in: Proc. of the IEEE International Conference on Network Protocols, ICNP, 2007.

[13] J. Deng, R. Han, S. Mishra, Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks, in: Proc. of IEEE International Conference on Dependable Systems and Networks, DSN, pp. 637–646, 2004.

[14] Y. Jian, S. Chen, Z. Zhang, L. Zhang, Protecting receiver-location privacy in wireless sensor networks, in: Proc. of IEEE INFOCOM, pp: 1955 – 1963, 2007.

[15] G. Chai, M. Xu, W. Xu, Z. Lin, Enhancing sink-location privacy in wireless sensor networks through k-anonymity, Int. J. Distrib. Sens. Netw. (2012).

[16] B. Ying, D. Makrakis, H.T. Mouftah, A protocol for sink location privacy protection in wireless sensor networks, in: Proc. of IEEE GLOBECOM, 2011.

[17] K.W. Tan, Y. Lin, K. Mouratidis, Spatial cloaking

revisited: distinguishing information leakage from anonymity, in: Proc. of the 11th International Symposium on Advances in Spatial and Temporal Databases, 2009.

[18] K. Mouratidis, M.L. Yiu, Shortest path computation with no information leakage, Proc. VLDB Endow. 5 (8) (2012) 692–703.

[19] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, ``Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Netw., vol. 7, no. 8, pp. 1501_1514, 2009.

[20] Jhumka, M. Leeke, and S. Shrestha, ``On the use of fake sources for source location privacy: Trade-offs between energy and privacy," Comput. J., vol. 54, no. 6, pp. 860_874, 2011.