International Journal of Engineering & Technology, 7 (3.27) (2018) 331-335

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Time Orient Trust Based Hook Selection Algorithm for Efficient Location Protection in Wireless Sensor Networks Using Frequency Measures

D. Prasanna[1*], R. Santhosh[2]

[1]Research Scholar, Department of CSE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
[2]Associate Professor, Department of CSE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.

Abstract

The presence of heavy adversary in the sensor network threats the quality of service hugely. To overcome the problem of location threat, a time orient trust based approach is presented in this paper. The method handles both source and sinks privacy by selecting random hook points around the region. The method identifies the list of sensors around its location and selects a single sensor as hook point based on the trust measure. The trust measure is estimated based on the participation of the sensor in other transmission and according to the energy parameters of the sensor node. The method uses two way protocols for route discovery.In the route discovery the hook point sends the route reply to the source node, which denotes a different route to be used. Similarly, the hook point fluctuates at each interval according to the frequency measures. For each hook point, the method computes the frequency measure based on the number of transmissions involved and the amount of data being received. The dynamic changing of hook point reduces the impact of heavy Eavesdroppers and improves the QoS of the network.

Index Terms: *WSN, Eavesdrop attack, location protection, hook selection, trust based selection, frequency measures, QoS.*

1. Introduction

The wireless sensor networks are becoming increasingly popular now because of its adaptability and rapid deployment support.

The modern mobile users access various services through their mobile devices and other PDAs. The services accessed by the mobile users are carried out by transmitting the data packets through intermediate sensor nodes. The sensor network is the collection of a number of sensor nodes to perform cooperative transmission. If there is a malicious node, then it will perform different network threats to the user service data. There are a number of malicious threats identified in the literature among them the Eavesdrop is the most critical threat.

Eavesdrop is the network threat being performed by a malicious node, which monitors the network traffic and simply discards the data packets without mercy. This highly affects the throughput performance of the network. There are different type of Eavesdroppers available. The low Eavesdropper is capable of monitoring the network traffic only within the region, whereas the higher Eavesdropper is capable monitoring the entire network traffic to perform Eavesdrop attack.

To safeguard the network servers and sink nodes, it is necessary to protect the sensitive information about the source and sink nodes. The sensitive pieces of information are energy, location and other information. A number of approaches are available for the protection of location information, but the heavy adversary is capable of reading the network traffic and identifying the location of the source and the sink.

Even though the Eavesdropper is capable of monitoring the data flow in the network, protecting the location information of the sink node is highly possible. Towards this issue, this paper presents a time orient hook selection algorithm. The hook is a sensor node, which is located around the sink and source node which has been selected in a dynamic manner.

The selection process has been carried out based on different metrics. Also, the hook is valid only for the current time window but will expire at the next time window. To select the hook, a number of parameters have to be considered.

First, the energy parameter has to be considered, because it would require to perform transmission of more number of data. Similarly, the sensor node must participate in the transmission of a limited number of data.

The frequency measure has to be used to validate the selection of the hook point. The trust measure would be used in validating the selection of the hook point. Each sensor node has to be validated for its trustworthy based on the number of data transmissions it has involved in the trace. Based on that, the method would verify whether it is a genuine sensor node or an Eavesdropper. It is necessary to verify the trustworthiness of the sensor node towards the heavy Eavesdropper.

Also, for the communication of control messages, the method adapts different routing protocols. The source node starts the route discovery but the reply comes from the hook point being selected at the time window. This will be varying at each time window, but the source would use a separate route to perform data transmission.

The Quality of service of the network has been approached using the time orient hook selection algorithm. By selecting the hook point in dynamic manner for each time window, the performance of the sensor network has been handled in efficient manner. The detailed approach is discussed in the next section.

2. Related Works

A number of approaches have been discussed for the problem of location protection and this section discusses various approaches towards the problem.

(KiranMehta) Protecting Location Privacy in Sensor Networks against a Global Eavesdropper [1], presents alocation privacy protection scheme towards Eavesdrop attack in WSN. The method introduces a lower overhead in communication to achieve location privacy. The method uses two different schemes to maintain the location of source nodes and sink nodes location in a secure manner. For both, it uses the simulation and backbone flooding techniques.

(Mauro Conti) Providing Source Location Privacy in Wireless Sensor Networks: A Survey [2], presents the source location privacy techniques. The paper classifies the methods based on the anonymization, un observation, capture likelihood and safety period. Also, various approaches are summarized to maintain the source location privacy.

(Yun Li, et al.) Preserving Source-Location Privacy in Wireless Sensor Networks [3], presented an location protection approach to maintain privacy of source location in both local and global level. The method uses (NMX) network mixing ring approach to provide global privacy in location of source. Also, to maintain the local privacy, an (RRIN) randomly routes intermediate node technique.

(Jia-Dong Zhang, et al.) REAL: A Reciprocal Protocol for Location Privacy in Wireless Sensor Networks[4], discuss a location protection approach to maintain the source location privacy in WSN.In this, the sensor nodes senses anonymized location with non-overlapping. The method uses a state transition algorithm, time delay approach with locking scheme to handle the reciprocal,accuracy and self-organization properties.

(Chinnu Mary George, et al.) Cluster based Location privacy in Wireless Sensor Networks against a universal adversary [5], discuss a cluster based approach to provide location privacy in the presence of global adversary. In this, context based and data based preservation technique is presented to handle the different attacks from the adversaries.

(Lin Zhou) The Location Privacy of Wireless Sensor Networks: Attacks and Countermeasures [6],analyzes different approaches of location protection and different measures being used to perform the task. Different models and their pros and cons have been discussed.

(Leron Lightfoot, et al.) Preserving Source-Location Privacy in Wireless Sensor Network Using STaR Routing[7], selects a neighbor randomly near the sink node to perform data transmission which is not too far and too close to the sink node.

(Chi-Yin Chow, et al.) A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks [8], discuss a two model location preservation scheme. The two model approach uses, resource aware algorithm to minimize the overhead produced in communication. The location is shared with the trusted persons located in the area. The quality algorithm maximizes the accuracy of the location privacy.

(Xi Luo, et al.) Location Privacy against Traffic Analysis Attacks in Wireless Sensor Networks[9], uses a randomly selected routing, where the algorithm generates dummy packets in different routes. This confuses the adversary and anonymous communication scheme has been used to provide location privacy.

(Arshad Jhumka, et al.)Towards Understanding Source Location Privacy in Wireless Sensor Networks through Fake Sources [10], uses a formalization technique to ensure the location privacy(Javier Lopez et al.). Preserving Receiver-Location Privacy in Wireless Sensor Networks [11], provide the sink level location privacy and traffic analysis approach.

(Lin Yao, et al.) Protecting the sink location privacy in wireless sensor networks[12], presents a two way routing algorithm with fake injection packets based location privacy. This increases the complexity of identifying the real sink for the adversaries. (Bi Di Ying et al.) Anti-traffic analysis attack for location privacy in WSNs [13], discuss an anti-traffic analysis based approach. In this approach, all the nodes generate dummy packets.

(Li Y, et al.) Quantitative measurement and design of source-location privacy schemes [14], presents an information leakage based approach. The method uses the quantitative leakage of source location detail for the route selection. Also, based on the measure, a random route selection algorithm is adapted.

(Mahmoud MMEA, et al.) A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks [15], presents a cloud based approach to safeguard the cloud locations against hotspot locating attack. The method generates an irregular shaped cloud with dummy traffic to deviate the adversary from genuine one.

All the methods struggled to achieve higher performance in location privacy and suffers from high network threat.

3. Time Orient Trust Based Hook Selection Algorithm

The proposed hook selection algorithm identifies the list of sensor nodes around the source and destination. For each sensor being identified, the method estimates the trust measure to perform hook selection. Similarly, the method estimates the frequency measures for hook selection and a detailed method is discussed in this section.

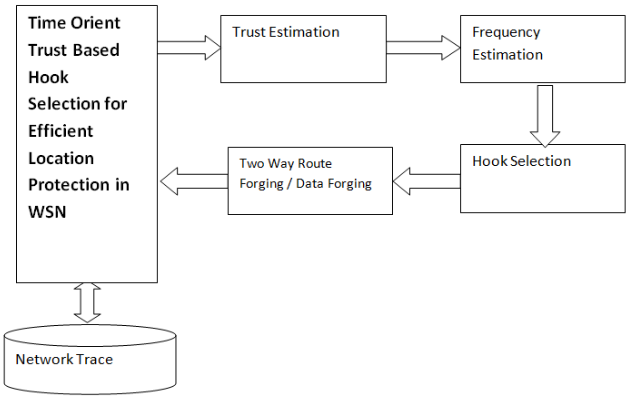
Time Orient Trust Based Hook Selection for Efficient Location Protection in WSN
Trust Estimation
Frequency Estimation
Hook Selection
Two Way Route Forging / Data Forging
Network Trace

Figure 1: Architecture of time orient trust based hook selection algorithm

Figure 1 shows the architecture of time orient trust based hook selection algorithm and the method involves various procedures to protect the location information of the sensor nodes.

Time Orient Trust Based Hook Selection

The hook selection algorithm first identifies the list of sensors around the source and destination. The sink node identifies the sensors and their physical characteristics like location, energy and so on.

Then for each sensor being identified, the method estimates the frequency and trust measures based on the previous transmission details. Based on the trust measure, a single hook point has been selected for data pooling. The data poured has been taken from the sensor node in another channel by multicasting to all its neighbors where the sink is one among them.

Algorithm

```
Input: Data packet Dp
Output: Null
Start
        Read Data Packet Dp.
        If Source then
                Identify list of sensors Ss = $\sum_{\mathrm{i=1}}^{\mathrm{size(TransmissionRange(S))}} \text{sensor} \in < Tr(s) >$
        For each sensor Si
            Trust Measure Tm = Estimate Trust Measure (Si)
            Frequency Measure Fm = Estimate Frequency Measure (Si)
            Hook s = Perform Hook Selection(Tm, Fm)
        End
        Perform TwoWay Route
    Else
        Identify list of sensors Ss = $\sum_{i=1}^{size(TransmissionRange(S))} sensor \in < Tr(s) >$
        For each sensor Si
            Trust Measure Tm = Estimate Trust Measure (Si)
            Frequency Measure Fm = Estimate Frequency Measure (Si)
            Hook s = Perform Hook Selection(Tm, Fm)
        End
        Perform Data Forging.
    End
Stop.
```

The algorithm discussed above computes the trust and frequency measures for different sensor nodes identified, which are located around the source or the sink node. Based on the measures estimated, the hook selection is performed. Through the selected hook sensor, the data transmission is performed. If it is a sink hook, then the hook node performs broadcast the packet in the network which has been received by the real sink node. The other nodes ignore the packet to complete the data transmission. For the next cycle, the sink node, selects the hook point and sends a control message in a two way route strategy to the source node.

4. Route Discovery

The proposed algorithm has major difference in the routing strategy. As the adversary monitors the data packets than control packets in major focus, in the routing procedure the exact protocol operations are decided. The source node sends the route discovery to the sink node by generating a route request. It has been flooded throughout the network. When a neighbor receives the message, it hands over the packet to the sink node itself.

The sink node performs the hook selection and places the sensor node to which it has to be handed over. The selected route has been used to perform data transmission, the packet will travel through the route upto the hook selected, when it reaches the hook. It will either multicast or broadcast the packet to the network, which can be received by the sensors located within the transmission range.

Algorithm

```
Input: packet P
Output: Null.
Start
    Read Packet P.
    Identify source S, Destination D.
    Generate Route request TH-RREQ.
    Broadcast RREQ in the network.
    Sensor receives the packet RREQ.
    If TH-RREQ(Source)$\in NeighborList$ then
        Send packet to Destination.
        Receive reply from Destination.
        Generate Route reply and send to the source node.
    End
    Source receives the reply.
    Extract the route and send data through the route.
    The hook present in the route receives the packet.
        Broadcast or multicast the packet.
    The sink receives the packet.
Stop.
```

I have indicated the route selection algorithm which discovers the route and uses a hook node to complete the data transmission, which has been selected in a dynamic manner which cannot be identified by the adversary easily.

Trust Estimation

It is more important to measure the trust of the node being selected to act as hook point. The sensor nodes participate in the transmission of a number of data. The genuine nodes come with limited energy and are capable of performing only a limited number of data transmission.

This is considered for the trust measurement. From the network trace, the method identifies the number of data transmissions the sensor node has been involved in and its average in all the cycles. Based on that its capability of completing the transmission based on the energy has been measured. Computed trust measure has been used to select the hook.

Algorithm

```
Input: Network Trace Nt, Sensor S
Output: Trust measure Tm
Start
    Read network trace NT
    Read sensor s.
    Identify the list of all transmissions performed by the sensor S.
    ST = $\sum_{i=1}^{size(NT)} NT(i).Route \in S$
    Compute Trust Measure Tm = ST×$\frac{\mu}{S.Energy}$
Stop
```

The algorithm discussed above, computes the trust measure for the sensor node identified and, based on the trust measure, the hook selection is performed.

Frequency Estimation

The hook selection should be performed in such a way that the adversary should not suspect the selected hook point. So the selected sensor should not be more frequent in the hook list. To perform this, the method computes the frequency of the sensor in hook list based on the network trace. Using the network trace, the method computes the number of transmissions it involved and number of times it acted as hook point. Based on these, the frequency measure has been estimated.

Algorithm

```
Input: Network Trace NT, Sensor S
Output: FM
Start
    Read network Trace Nt.
    Read sensor s.
    Identify the list of all transmissions performed by the sensor S.
    ST = $\sum_{i=1}^{size(NT)} NT(i).Route \in S$
    Identify number of times it has been acted as hook.
```

$Ht = \sum_{i=1}^{size(NT)} NT(i).Route.Dest == S$

Compute frequency measure $FM = \frac{Ht}{St} \times \frac{Ht}{size(Nt)}$

Stop

The algorithm discussed above, computes the frequency measure based on the transmissions involved by the sensor node and has been used to perform hook selection.

5. Hook Selection

The hook selection is the major part of the protocol being designed. If there is a set of sensors Ss, each has various frequency and trust measures according to the previous data transmission.

The sensors located around the sink node is considered for the hook selection. According to this, the protocol selects the hook node as follows:

Identify list of sensors present around the sink node as follows:

$Asl = \sum Sensors(Network)@sink$

Now for each sensor identify the location and region according to sink.

Location $l = \int_{i=1}^{size(Asl)} Asl(i).location$

Region $R = \int_{i=1}^{4} Region(i) \in L$

Now for each sensor compute trust measure Tm.

Now for each sensor compute frequency measure Fm.

Identify the previous hooks region Ph.

Identify the list of sensors not present in previous region.

Sensor list $Sl = \sum Sensors(Asl) \nexists Region(Ph)$

For each sensor s from Sl

Compute Hook support $Hs = \int_{i=1}^{size(Sl)} Sl(i).Tm \times Sl(i).Fm$

End

Choose the hook with higher support H.

The hook sensor has been selected based on the hook support measure which has been estimated based on the frequency and trust measures.

Two Way Route Forging and Data Forging

The method performs routing of the packets in two modes. When a route discovery packet is received, the sink node identifies the route and hook node for the data transmission. The route reply will contain the information about the route to be used for data transmission and the hook to which the packets have to be sent. Similarly when the hook node receives the data packet belonging to the sink node, it broadcasts or multicasts the packet in the network. In case of multicasting, it selects more number of sensors with the original sink.

The other node ignores the packet, but the original sink receives the data packet properly.

6. Results and Discussion

The proposed time orient trust based hook selection algorithm has been implemented and evaluated for its efficiency.

The hook selection algorithm has been implemented using advanced java.

The algorithm has been tested with various simulation scenario and validated for its efficiency.

Table 1: Details of Simulation

Parameter	Value
Tool Used	Advanced Java
No of nodes	200
Protocol	TTH
Simulation Time	10 Minutes

Table 1 shows the simulation details being used to evaluate the performance of the proposed algorithm. [16]

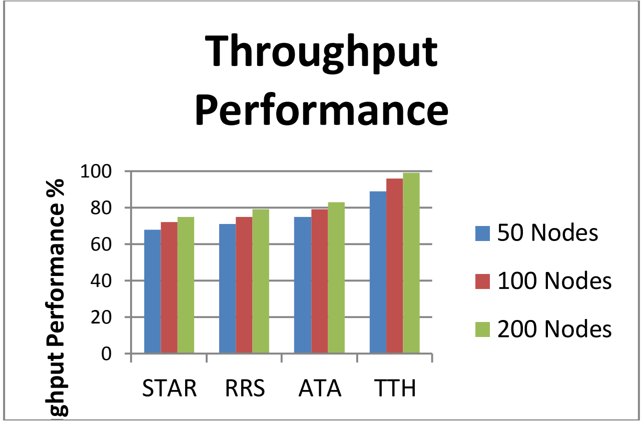

Figure 2: Comparison on throughput performance

The Figure 2 shows the comparison on throughput performance produced by different methods. The Proposed TTH algorithm has produced higher throughput performance than other methods in all the simulation scenario considered.

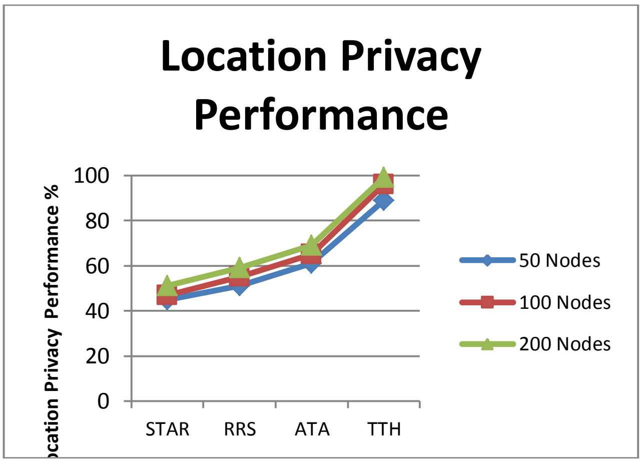

Figure 3: Comparison on location privacy performance

The Figure 3 shows the comparative result on location privacy produced by different methods. The proposed TTH algorithm has produced higher location privacy performance than other methods.

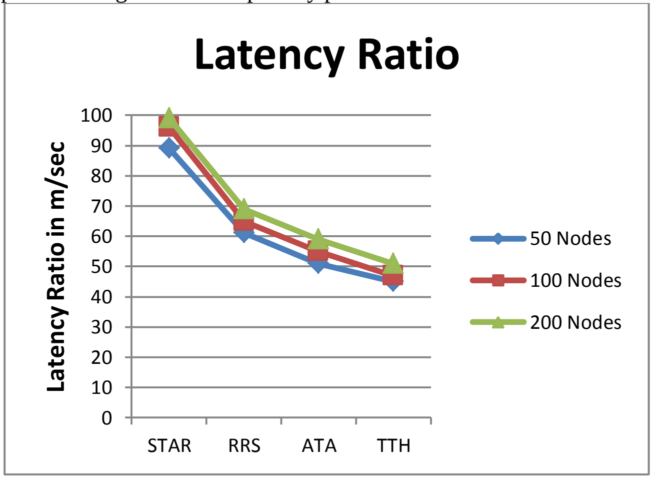

Figure 4: Comparison on latency ratio

Figure 4 shows the comparison on latency produced by different methods. The proposed TTH algorithm has produced less latency ratio compared to other methods.[17]

7. Conclusion

In this paper, an efficient time orient trust based hook selection algorithm is presented. The method selects a hook point for the sink node at each time window. The hook node is selected based on the trust measure and frequency measures of the neighbor sensors. For each sensor node available near the sink node, the measures are estimated and based on that a hook weight has been measured. At each time window, the hook selection is performed not only based on the weight but also based on the region where the hook is located. At each time window the hook selection is performed according to the region and it has been maintained in such a way that the subsequent hooks are not present in the same region. The packets are routed in dual mode so that the adversary cannot identify the original sink. The proposed method improves the performance of location privacy and improves the throughput performance.

References

[1] Mehta K, Liu D & Wright, M, “Protecting location privacy in sensor networks against a global eavesdropper”, *IEEE Transactions on Mobile Computing*, Vol.11, No.2, (2012), pp.320-336.

[2] Conti M, Willemsen J & Crispo B, “Providing source location privacy in wireless sensor networks: A survey”, *IEEE Communications Surveys & Tutorials*, Vol.15, No.3, (2013), pp.1238-1280.

[3] Li Y & Ren J, “Preserving source-location privacy in wireless sensor networks”, *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, (2009), pp.1-9.

[4] Zhang JD & Chow CY, “REAL: a reciprocal protocol for location privacy in wireless sensor networks”, *IEEE Transactions on Dependable and Secure Computing*, Vol.12, No.4, (2015), pp.458-471.

[5] George CM & Kumar M, “Cluster based Location privacy in Wireless Sensor Networks against a universal adversary”, *IEEE International Conference on Information Communication and Embedded Systems (ICICES)*, (2013), pp.288-293.

[6] Zhou L, Wan C, Huang J, Pei B & Chen C, “The location privacy of wireless sensor networks: Attacks and countermeasures”, *IEEE Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, (2014), pp.64-71.

[7] Lightfoot L, Li Y & Ren, J, “Preserving source-location privacy in wireless sensor network using STaR routing”, *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, (2010), pp.1-5.

[8] Chow CY, Mokbel MF & He T, “A privacy-preserving location monitoring system for wireless sensor networks”, *IEEE Transactions on Mobile Computing*, Vol.10, No.1, (2011), pp.94-107.

[9] Luo X, Ji X & Park MS, “Location privacy against traffic analysis attacks in wireless sensor networks”, *IEEE International Conference on Information Science and Applications (ICISA)*, (2010), pp.1-6.

[10] Jhumka A, Bradbury M & Leeke M, “Towards understanding source location privacy in wireless sensor networks through fake sources”, *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, (2012), 760-768.

[11] Lopez J, Rios R & Cuellar J, “Preserving receiver-location privacy in wireless sensor networks”, *International Conference on Information Security Practice and Experience*, (2014), pp.15-27.

[12] Yao L, Kang L, Shang P & Wu G, “Protecting the sink location privacy in wireless sensor networks”, *Personal and ubiquitous computing*, Vol.17, No.5, (2013), pp.883-893.

[13] Di Ying B, Makrakis D & Mouftah HT, “Anti-traffic analysis attack for location privacy in WSNs”, *EURASIP Journal on Wireless Communications and Networking*, (2014).

[14] Li Y, Ren J & Wu J, “Quantitative measurement and design of source-location privacy schemes for wireless sensor networks”, *IEEE Transactions on Parallel and Distributed Systems*, Vol.23, No.7, (2012), pp.1302-1311.

[15] Mahmoud MM & Shen X, “A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks”, *IEEE Transactions on Parallel and Distributed Systems*, Vol.23, No.10, (2012), pp.1805-1818.

[16] G Abilbakieva, M Knissarina, K Adanov, S Seitenova, G Bekeshova (2018). Managerial competence of future specialists of the education system (Preschool education and upbringing) and medicine in the comparative aspect. Opción, Año 33, No. 85. 44-62.

[17] Akhpanov, S. Sabitov, R. Shaykhadenov (2018). Criminal pre-trial proceedings in the Republic of Kazakhstan: Trend of the institutional transformations. Opción, Año 33. 107-125.