International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-6, June 2015

Analysis of DREAM Protocol to enhance source and sink location privacy against eavesdropper in WSN

Gurwinder Singh, Nitin Bhagat

Abstract— **Wireless Sensor Network's (WSN) location privacy protection is an important issue. In this paper, we address the necessity of concurrently protecting the location privacy of both the source and sink. We propose Dream Protocol to deliver messages from source to sink, which can protect the end-to-end location privacy against the local eavesdropper. We also implemented this scheme on the ns-2 platform, and evaluate the performance in terms of end-to-end latency and energy consumption. The results illustrate that our proposed privacy protection schemes can obtain satisfied performance. Our proposed scheme has analyzed the location privacy protection at the source and sinks respectively. We have designed an optimal combination scheme to achieve a highest location privacy protection for both ends.**

***Index Terms*— WSN, DREAM protocol, sensor network security, local eavesdropper, location privacy.**

I. INTRODUCTION

With a increased area of the applications of WSN, the security mechanisms are rising issue of outmost concern. The most important challenges threatening the successful installation of sensor systems is its privacy. Many privacy-related issues has been addressed by security mechanisms, but one sensor network privacy issue that cannot be adequately addressed by network security is source-location privacy One important class of sensor-driven applications is to monitor a valuable resources. For instance, sensors will be deployed in places like natural habitats to monitor the activities of endangered animals, or may be used in military purposes. In these asset monitoring applications, it is important to provide security to the source sensor's location [6]. Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. The main characteristics of wireless sensor network include [9]:

- Power consumption constrains for nodes using batteries or energy harvesting
- Capability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale deployment
- Ability to withstand harsh physical conditions
- Ease of use

Gurwinder Singh, CSE, Punjab Technical University, Jallandhar, India, 9988866636.
Nitin Bhagat, CSE, Punjab Technical University, Jallandhar, India.

A. Applications

Sensor networks can be used for wide range of applications where it is difficult or infeasible to set up wired networks. Examples include wildlife habitat monitoring, security and military surveillance, and target tracking [4].

Wireless Sensor Network applications are divided into two categories [8]:

1) *Event Detection:* In this, the aim of deploying the sensor nodes is to detect and inform about an event to the sink nodes. The emphasis is on deploying the nodes with simple signal processing capabilities and to keep the number of sensor nodes to be sufficient to detect an event but they must avoid the false alarms. The examples of event detection applications are detection of fire in a forest or an earthquake.
2) *Spatial Process Estimation:* In this, the aim is to estimate a physical phenomenon which can be modeled as bi-dimensional random process. The entire behavior of the spatial process is estimated by receiving the samples from the sensor nodes which are deployed at the random locations.

B. Types of attacks

There are many types of attacks that can happen in the wireless sensor network (WSN). Some of them are discussed as follow [1]:

1) *Selective Forwarding:* In this, a malicious node attacks the network. It than captures a node from it and drops some packets of data. This type of attack becomes crucial when the attacker collects traffic information through the captured node.
2) *Hotspot-Locating Attack:* The local eavesdropper collects data about traffic in the network. Then it analyzes this data through traffic analysis techniques. It than locates the hotspots so that it can attack on these places.
3) *Sinkhole Attack:* Sinkhole attack is a kind of attack in which the attacker tries to draw focus of the traffic to a specific node so that it can steal the data from the network.
4) *Source Location Attack:* In this attack, the attacker attempts to locate the source node by using the traffic of the network. If the attacker is able to find the source node, than it can easily attack the network and steal the data or it may halt the network.

II. RELATED WORK

Kumar et al. [2] analyzes all the routing protocols and proposes DREAM protocol over the other protocols. In this paper, we discuss the DREAM protocol for routing. DREAM stands for Distance Routing Effect Algorithm for Mobility. It is a location based routing protocol in which each node sends

updated location to every other node. Each node contains a routing table which contains the geographical location of all other nodes in the network. Sharing of geographical location data reduces the bandwidth consumption in the network. So, it is one of the advantages of using DREAM protocol over the other protocols. Also the stationary nodes need not to send the updated location messages because they move slowly as compared to other nodes.

Bakhouya et al. [3] evaluates DREAM protocol. DREAM protocol implements two algorithms. In first, the location information packets are distributed and in second, the data packets are disseminated. The first algorithm is based on restricted flooding idea. To restrict the flooding, the maximum distance is defined that a position packet can travel. Principle of distance effect is also used in which the location table update frequency is determined by the distance of registered nodes. The closer the node, the more updates sent to it. Thus nodes departing far away normally have a more stable relative location relationship. As a result when a node maintains the location information of another node that is far apart, less frequent updates are used. In second algorithm, the data packets are disseminated using directional flooding where the source forwards the packet to all one hop neighbors that are lying in the direction of destination. To determine the forwarding zone in the direction of destination, the source node calculates the region that is likely to hold destination, called the Expected Region. When the source node wishes to send a message to a destination node, the position table is checked to retrieve information about its geographical position. If the direction of destination is valid, the message is forwarded by source to the all one hop neighbors in the forwarding zone using that direction. In case no one hop neighbor is found in the required direction i.e. no location information is available for destination, then a recovery procedure is started by flooding partly or totally the network in order to reach destination. When any node receives the data packet and it itself a destination, an acknowledgement is replied back to the source node regarding message receiving, otherwise all other nodes except destination replicate the same method by sending it to all one hop neighbors that are in the direction of destination. This method is replicated by each of these nodes, until destination is reached.

Pavitha et al. [4] states that many of the protocols used to provide sensor network security provide confidentiality for the content of the messages but contextual information usually remains exposed. Such contextual information can be misused by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. Existing techniques protect the leakage of location information from a limited adversary who can only observe network traffic in a small region. However, a stronger adversary, the global eavesdropper, is realistic and can overthrow these existing techniques.

Choudhary et al. [5] said that wireless sensor network (WSN) has been proposed for many useful applications for automatic data collecting such as habitat monitoring, military surveillance, home and business smart environments, better management of cities in areas like traffic control, intelligent transportation, search and rescue, disaster relief, and target tracking, for monitoring the activities of enemy soldiers or valuable assets, e.g., endangered animals. This research considered habitat monitoring applications where the WSN is deployed for monitoring pandas. For example, a WSN has been deployed by the Save-The-Panda Organization to monitor pandas in a wild habitat. While pandas move in the network, their presence and activities are periodically sensed by the sensor nodes and reported to the Sink. However, WSNs are usually deployed in open and large areas that are unattended and lack of protected physical boundary, which makes the networks vulnerable to many threats.

Wadhwa et al. [7] reviews that DREAM is an early example of a routing protocol which is completely location-based. The location service is also part of the same protocol. With DREAM's location service, every node proactively updates every other node about its location. The overhead of such location updates is reduced in two ways. First, distance effect (nodes move slowly with respect to each other as their distance of separation increases). Second, each node generates updates about its location depending on its mobility rate| fast moving nodes update more often whereas slow moving nodes generate updates less often.

III. Results Analysis

Fig. 1 shows the end-to-end latency comparison for our proposed scheme and the various previous schemes. For the Dream Protocol scheme, as the actual messages are delivered along the Dream Protocol from source to sink, they would achieve the shortest end-to-end latency. Since the actual messages in the DBT Schema and FRW are same. Their delivery latency work at same level. Also the results values show it is same for BT and ZBT schemes because they are following the shortest path. When the hop count equals to 15, the end-to-end latency of the ZBT scheme is the Highest as they uses the ZIG ZAG path to mislead the adversary. When the hop count is larger than 15, the end-to-end latency of the FRW and DBT exceeds that of the ZBT scheme. The result of graph shows the efficiency of Proposed Schema is efficient than previous schema.

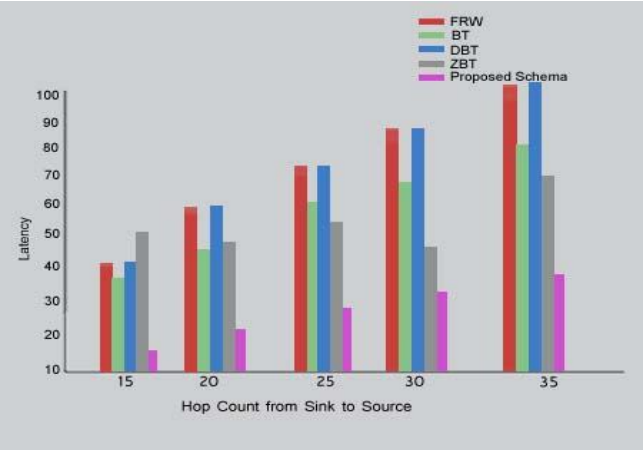

Fig. 1 Latency comparison graph

Table (198) shows latency comparison of various schemas with proposed schema. The result of proposed schema are efficient than previous schema.

Table (198): Values of Latency

Hop Count	FRW	BT	DBT	ZBT	Proposed Schema
15	40	38	40	50	15
20	55	42	55	45	20
25	70	52	70	42	23
30	82	55	82	42	30
35	100	60	100	62	35

Table (199) shows energy consumption comparison of various schemas with proposed schema. The result of proposed schema are efficient than previous schema.

Table (199): Values of Energy Consumption

Hop Count	FRW	BT	DBT	ZBT	Proposed Schema
15	40	110	140	180	20
20	70	180	180	200	27
25	100	200	220	200	30
30	120	230	300	160	38
35	140	260	350	300	42

Fig. 2 shows the comparison graph of energy consumption of the previous four schemes and our proposed scheme. The efficiency of our proposed schema Dream Protocol scheme achieves the highest performance with lesser energy consumption while the other schemes have the more energy consumption. As it is more time-consuming for the adversary to capture the sink than the source, the safety period of the sink location privacy is also larger than that of the source location privacy.

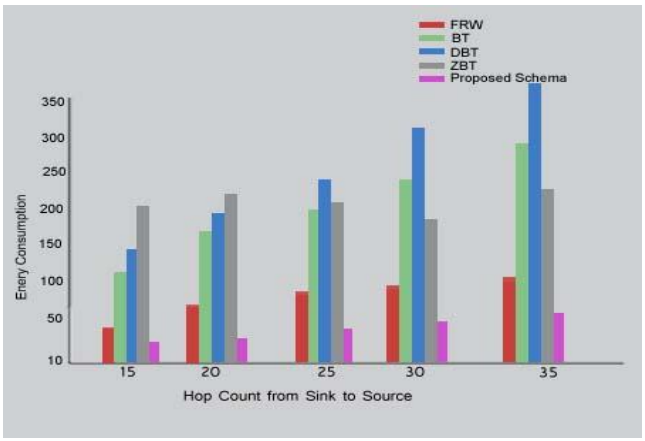

Fig. 2 Energy Consumption comparison graph

IV. CONCLUSION

The end-to-end location privacy is an important issue in WSNs. In this we address the necessity of simultaneously protecting the location privacy of both the source and sink in the habitat monitoring system. We propose Dream Protocol Scheme, to deliver messages from source to sink, which can protect the end-to-end location privacy against the local eavesdropper. We also implement the proposed schemes on the ns-2 platform, and evaluate the performance in terms of safety period, end-to-end latency and energy consumption. The results illustrate that our proposed location privacy protection schemes can obtain satisfied performance, as our proposed schemes have analyzed the location privacy protection at the source and sink respectively. We have designed an optimal combination schemes to achieve a highest location privacy protection for both ends. In our future work, we will focus on extending our scheme to be applicable to work efficiently if the number of nodes is increased with less latency and lesser energy consumption.

REFERENCES

[1] V. Gobinath, K. Bergin Shyni, "SECURING SOURCE-LOCATION FROM HOTSPOT-LOCATING ATTACK IN WSN" IJARSE, Vol. 4, Special Issue (02), March 2015.
[2] Puneet Kumar, Dr. Ashish Kumar, "Simulation Based Analysis of DSR, LAR and DREAM Routing Protocol for Mobile Ad hoc Networks" MIT International Journal of Computer Science & Information Technology, Vol. 3, No. 2, August 2013, pp. 58–62.
[3] Bakhouya, J. Gaber, M. Wack, "Performance evaluation of DREAM protocol for Inter-Vehicle Communication" 1st Intl. Conference on Wireless Communications, Vehicular Tech, Information Theory, and Aerospace & Electronic Systems Technology, Wireless VITAE 2009, pp. 289-293, Aalborg, May 2009.
[4] Pavitha N, S. N. Shelke, "Providing Source and Sink Location Privacy against a Global Eavesdropper in Sensor Networks: a Survey" International Journal of Research (IJR), Vol. 1, No. 2, July 2014.
[5] Anupam Choudhary, Sapna Choudhary, Nidhi Patel, "A Survey Paper of Various Attack in Wireless Sensor Network" International Journal of Advance Research in Computer Science and Software Engineering (IJARCSSE), Vol. 1, No. 5, March 2015.
[6] Neha Sahu, Sanjay Sharma "A Deviated Location and Updated Node Identity based Security Scheme for Preserving Source Node Location Privacy in Wireless Sensor Network" International Journal of Computer Applications, Vol. 100, No. 5, Aug 2014.
[7] Divya Wadhwa, Deepika, Vimmi Kochher, Rajesh Kumar Tyagi "A Review of Comparision of Geographic Routing Protocols in Mobile Adhoc Network" Advance in Electronic and Electric Engineering, Vol. 4, November 2014, pp. 51-58.
[8] Pooja Chaturvedi, A. K. Daniel, "Wireless Sensor Networks-A Survey" ACEEE, 2014.
[9] Priti C. Shahare, Nekita A. Chavhan, "Secure and Efficient Sink Node Location Privacy Technique in WSN" International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 3, March 2014.