Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.610 – 616

EAACK-A Secure Intrusion Detection System for MANET: SURVEY

Sumaiya Rashid, Sumit Wadhwa
rashidsumaiya10@gmail.com, sgisumitcse@gmail.com
Samalkha Group of Institutions Samalkha, NH-1, Delhi NCR, 132115(HR.)

ABSTRACT: The privacy issue, especially location privacy, can be critical for monitoring applications in WSNs. A unique case of location privacy is that of the sources, which are vulnerable of being captured and target attacks. Wireless sensor networks (WSNs) have many promising applications for monitoring critical regions, such as in military surveillance and target tracking. In such applications, privacy of the location of the source sensor is of utmost importance as its compromise may reveal the location of the object being monitored. Traditional security mechanisms, like encryption, have proven to be ineffective as location of the source can also be revealed by analysis of the direction of traffic flow in the network. Due to the open nature of a sensor network, it is relatively easy for an adversary to eavesdrop and trace packet movement in the network in order to capture the source and destination physically. Many security protocols have been developed to provide confidentiality for the content of messages whereas contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. This paper is a survey of various techniques to provide location privacy in sensor network. We have analyzed various techniques to provide location privacy for source node and also for sink node.

Keywords: source, sink, wsn, location privacy.

I. INTRODUCTION

Source Location Privacy (SLP) is mostly perceived as part of context privacy and aims at hiding the (location of the) source node from the adversary. There are multiple metrics to evaluate the effectiveness of the given SLP: the safety period, and the capture likelihood are key. Many works use privacy entropy as a metric to measure the quality of the delivered SLP. In some applications the measure of distance error is used to measure the quality of the delivered SLP. Anonymity and unobservability are directly related to SLP. The anonymity and unobservability of a solution can be measured by the delivered size of the anonymity sets and unobservability sets. Another metric for anonymity is the use of the effective size of an anonymity probability. The statistical source anonymity can be combined with event unobservability to provide SLP. There are various taxonomies that use a different name for SLP. We already mentioned SLP as part of contextual privacy. Contextual privacy relates identity privacy, timing privacy, and route privacy to SLP. Some authors use a different taxonomy for context privacy: they only identify location privacy and temporal privacy as part of context privacy. Some refer to SLP as data source location privacy, whereas other authors refer to SLP from a network level perspective. From the network level perspective, SLP is defined as part of network level privacy and is named sender node location privacy. Another taxonomy that is used in the state of the art, is the one of transactional confidentiality, which is essentially the same as context privacy. There are number of the applications in the WSN. This includes [1] the military applications which controls the monitoring, tracking and surveillance of the borders. Other applications include the environmental applications, health applications, home applications, commercial applications. WSN are capable to collect their data automatically with the help of the sensor devices. Even though there is great benefit to the users some misuse them so privacy is a concern there. If we take famous scenario of the panda and hunter [2], the hunters can physical location of the panda by monitoring the traffic or using sound monitoring where in panda is tracked with help of the sound recognition. So a design of the new technologies should be taken into account against privacy. In this paper a review of the existing privacy techniques in WSN has been presented. There are two main categories of the privacy preserving techniques; data privacy and context oriented privacy. The data privacy focuses on privacy of the data so that no modification is done to the data. The context oriented privacy focuses on the contextual information this includes the location information or time of the event. This paper is with respect to the context oriented privacy. In context oriented privacy we focus on the location privacy. At the end some issues are presented which would be helpful for future research in privacy in WSN.

II. SECURITY ISSUES IN SENSOR NETWORK

Privacy is one of the most important problems in wireless sensor networks due to the open nature of wireless communication, which makes it very easy for adversaries to eavesdrop. When deployed in critical applications, mechanisms must be in place to secure a WSN. Security issues associated with WSNs can be categorized into two broad classes: content-related security, and contextual security. Content-related security deals with security issues related to the content of data traversing the sensor network such as data secrecy, integrity, and key exchange. Numerous efforts have recently been dedicated to content-related security issues, such as secure routing, key management and establishment, access control, and data aggregation. In many cases, it does not suffice to just address the content-related security issues. Suppose a sensitive event triggers a packet being sent over the network; while the content of the packet is encrypted, knowing which node sends the packet reveals the location where the event occurs. Contextual security is thus concerned with protecting such contextual information associated with data collection and transmission.

One of the ways to increase the reliability and range of the WSNs is to employ multi-hop routing. The concept of multi-hop routing is to forward a packet to the destination using different path in case of the node failure. But, the critical issue still remains of providing security and privacy in WSNs. Therefore, preserving location privacy of the source node remains critical. Wireless sensor networks are used in many areas such as military supervision where possibility of the eavesdropping the traffic is high to get hold of sensitive information. Exploitation of such information can cause economic losses or cause danger to human lives. To protect such information, researchers are finding out new ways to provide standard security services such as, availability, integrity, confidentiality and authentication. The exchange of information between sensors can disclose sensitive information which can reveal the location information of the critical modules present in the network.

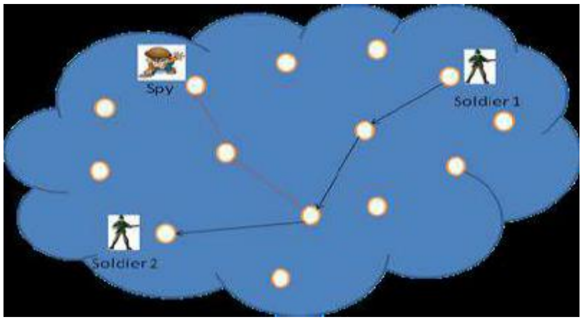

Figure 1.Threates in military surveillance

The figure 1 shows WSNs deployed in the military observation area. In this figure the soldier 1 is sending some trusted data to the soldier 2 via many intermediate nodes. Here soldier 2 is the sink node. A spy who is present on the same network tries to intercept the data by negotiating one of the intermediary nodes. The nodes may reveal trusted data to the adversary such as location of the source, location of the sink or positions of the armed forces in the locality.

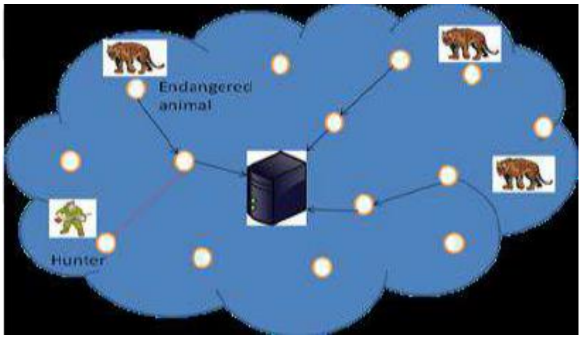

Figure2: Threats in monitoring endangered animals

The figure 2 shows the deployment of sensor network to monitor the endangered animals in a forest. An event is generated whenever an animal is spotted in the monitored area. The hunter tries to gather this information and may capture or kill the endangered animal. The above scenario depicts the vulnerability of WSNs is more because of its open wireless medium to transmit the information from source to destination.

III. PRIVACY PRESERVING TECHNIQUES

This section deals with two most important branches of the privacy preservation techniques data oriented privacy and context oriented privacy. Data oriented privacy focuses on the data that is being collected and then send to the sink. Context oriented privacy is the contextual information like that of the physical location or time of the event.

3.1 Context oriented privacy preservation techniques

Although privacy is achieved with different protection techniques, the sensor nodes are so sensitive that it needs to be protected. The adversary can use traffic analysis techniques [3]. Context oriented privacy is summarized in the next two sections.

3.2 Location privacy

Location privacy is a critical issue in WSN especially in the case of the hostile environments. Failure to such physical location can subvert and disable the network there by allowing the adversary to launch attacks. The famous panda hunter problem [2] where in the sensor are deployed in the forest. Sensor nodes are used to find the physical location of the panda in their local habitat. Adversary can find the location of the sensor node that monitor the panda and thereby capture the panda. Location privacy is further classified into two main categories; location privacy of data source and location privacy of data sink

3.2.1 Location privacy for the data source

Suppose we take a scenario of the famous panda hunter problem where in sensors are being deployed in the forest. The hunters are monitoring and thereby capturing the panda. A sensor node detects the presence of the panda and sends to the base station with the help of the multihop communication while rest of the sensor nodes being idle. The hunter now sees that the base station has received the presence of the panda and would like to know the exact source. The hunter can use the backtracking procedure or the traffic analysis and find the exact location of the data source. So privacy protection is needed at the data source.

Flooding [4] has been used to preserve the physical location of the data source .In the case of the baseline flooding mechanism. a sensor node detects the presence of the panda and broadcasts it to its neighbors. These neighbors in turn broadcast to their neighbor and finally being received by the base station. The hunter notices that the base station receives multiple copies of the same message. And thereby confusing the hunter or the adversary. However the effectiveness of the base lining flooding depends on the no of nodes on the transmission path between the data source and base station. If the path is too short then the hunter can use the shortest path between the data source and base station. To address the consequence of the baseline flooding, probabilistic flooding is proposed in [4], in this mechanism not all sensors are involved in the forwarding data rather each node broadcasts with a Preset probability .This scheme reduces the energy consumption but there is no guarantee of the reception data by the base station due to the randomness involved this mechanism. Higher level of privacy can be achieved with the help of the random walk mechanism [4] where in phantom routing is used. In this a random walk is performed from the data source, and then a probabilistic flooding scheme is then used.fig3 Shows the random walk mechanism.

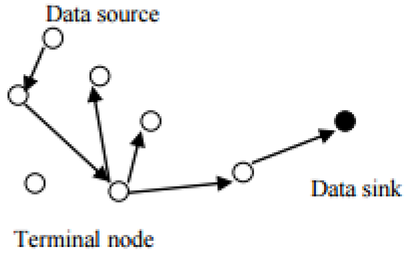

Figure 3:Random walk Machenism

Another higher level technique is the greedy random walk [5] where in the base station first initializes a random path with a given number of the hops. Sensors on this particular path are called the receptors. Then a packet is randomly forwarded from the data source until they reach one of the receptors. Thereby then following the pre established path by the base station. Fig4. shows the greedy walk mechanism.

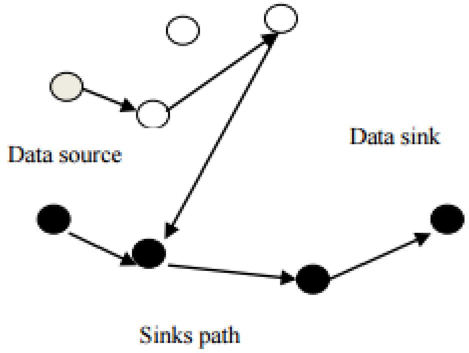

Figure 4: Greedy walk Mechanism

To further protect the physical location of the data source dummy data mechanism is used. In this fake packets are introduced to disturb the traffic .a simple scheme of the short lived fake source routing is proposed [4] where in each sensor sends a fake packet with a pre-determined probability. Upon receiving a fake packet, a sensor node just discards the packet and upon receiving the real packet it forward to the base station. However energy efficiency is maintained but the length of the each path for the fake path is one hop. Therefore the hunter or the adversary can discard the fake paths and reach to the physical location of the data source. A still higher level of privacy is achieved with the help of the fake sources mechanism [6]. In this mechanism one or more sensor nodes are chosen to simulate the behavior of the real data source in order to confuse the adversary. However the power consumption is quite high.

3.2.2 Location privacy for base station

Since base station collects the entire data from the network so location privacy is needed at the data sink. Suppose the scenario of the military application where in the soldiers are equipped with the sensors. The soldiers detects the presence of the enemy and send it to the base station using multihop communication , now the adversary notices that the base station receives large amount of the traffic and there by decides to destroys the base station and thus disabling the whole network . Hence the protection of the base station is very important. There are different traffic analysis techniques [7] .This includes the time correlation attack where in the adversary observes the correlation in the sending time between a node and the neighbor node who is assumed to be forwarding data and then deduces the path to the base station. Another technique is rate monitoring attack where in the adversary monitors the packet sending rate of the nodes and then moves closer to the nodes that have highest packet sending rate. Another privacy technique is the differential fractal propagation technique, where in a sensor node sends a real packet, its neighbor node generates the fake packet. The fake packet then travels a given number of the hops. They also design a scheme for creating some areas of the high activity called the hotspots. If such an area receives a packet it creates a high area of the activity and there by local eavesdropper being deceived to this area. But the packet may not be necessarily in this area. And thereby the adversary being confused.

Another approach is the location privacy routing protocol that provides privacy protection to the destination with a given number of the hops also fake packets are generated to the destination .the packets may move close either closer or away from the destination .the fake packets are generated so as to confuse the adversary. Yet higher level of privacy is achieved with the help of the hop by hop encryption technique where in data encryption technique the packet is re-encrypted hop by hop when its transmitted to the base station. Thereby by not disclosing the base station location through changing the appearance of the data .Yet higher level of privacy is achieved with the help of the hop by hop encryption technique where in data encryption technique the packet is re-encrypted hop by hop when its transmitted to the base station. Thereby by not disclosing the base station location through changing the appearance of the data.

IV. COMPARISONS

In this we compare all the privacy preserving techniques that have been reviewed in this paper the performance of privacy preservation techniques in WSNs. We evaluate their performances in metrics: privacy, accuracy, delay time, and power consumption, location, adversary, message overhead, scalability. Privacy refers to the degree of privacy protection provided by the reviewed techniques. The accuracy measure covers two perspectives: (i) the accuracy of the data obtained by the base station; and (ii) the availability of the (intended) data to the base station (i.e., whether the data can be delivered to the base station). The delay time includes both the computation and communication time of data transmission at the intermediate sensors. The power consumption measure focuses on the additional messages required for transmission (i.e., additional energy consumed) in the WSN. There are some open issues for future research. As the network behavior changes so sensor nodes should be designed accordingly, along with it there can be improvement in every technique with respect to overhead, power, accuracy.

V. CONCLUSION

Providing privacy for contextual information such as location of the source or sink node is very important in sensor network. An adversary can use location information and perform some attacks on either source node or destination node. In this paper, we have studied different approaches for providing location privacy for source node and sink node against adversaries in sensor network. This paper presents a review of privacy-preserving techniques for wireless sensor networks (WSN) . Two main categories of privacy preserving techniques have been presented; data oriented and context oriented respectively. The existing techniques have been compared in terms of context privacy preservation with respect to efficiency, overhead, delay, power consumption adversary, location, scalability against a local eavesdropper. In future these techniques can be modified and can be used to protect against a global eavesdropper who has a global view of the traffic at a time.

REFERENCES

[1] K. Sohraby, D. Minoli and T. Znati. , “Wireless Sensor Network: Technology, Protocols and Applications:” John Wiley & Sons, 2007,pg10-11.

[2] C. Ozturk, Y. Zhang, and W. Trappe. “Source-location privacy in energy constrained sensor network routing”: In Proceedings of the 2nd ACM workshop on Security of Adhoc and Sensor Networks, 2004

[3] Jean-Franois Raymond. Traffic analysis: Protocols, attacks, design issues and open problems. In Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, pages 10-29. SpringerVerlag New York, Inc., 2001.

[4] Celal Ozturk, Yanyong Zhang, and Wade Trappe, “Source location privacy in energy-constrained sensor network routing”. In SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pages 88-93, New York, NY, USA, 2004. ACM.

[5] Y. Xi, L. Schwiebert, W.S. Shi, Preserving source location privacy in monitoring-based wireless sensor networks, in: Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), April 2006.

[6] K. Mehta, Donggang Liu, and M. Wright. “Location privacy in sensor networks against a global eavesdropper”. In IEEE International Conference on Network Protocols, 2007. ICNP 2007, pages 31-323, October 2007

[7] Jing Deng, Richard Han, and Shivakant Mishra. Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. In DSN '04: Proceedings of the 2004 International Conference on Dependable Systems and Networks, pages 637-646, Washington, DC, USA, 2004.IEEE Computer Society