International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2016 IJSRCSEIT | Volume 1 | Issue 1 | ISSN : 2456-3307

Temperature analysis with respect to time maintenance in a WSN

A. Rameez Noorjahan Fathima*, K. Sugasini

Department of Computer Science and Engineering, Anna University/IFET College of Engineering/ Villupuram, TamilNadu, India

ABSTRACT

We address the problem of preventing the inference of contextual information in event-driven wireless sensor networks (WSNs). The problem is considered under a global eavesdropper who analyzes low-level RF transmission attributes, such as the number of transmitted packets, inter-packet times, and traffic directionality, to infer event location, its occurrence time, and the sink location. We devise a general traffic analysis method for inferring contextual information by correlating transmission times with eavesdropping locations. Our analysis shows that most existing countermeasures either fail to provide adequate protection, or incur high communication and delay overheads. To mitigate the impact of eavesdropping, we propose resource-efficient traffic normalization schemes. In comparison to the state-of-the-art, our methods reduce the communication overhead by more than 50%; and the end-to-end delay by more than 30%. To do so, we partition the WSN to minimum connected dominating sets that operate in a round-robin fashion. This allows us to reduce the number of traffic sources active at a given time, while providing routing paths to any node in the WSN. We further reduce packet delay by loosely coordinating packet relaying, without revealing the traffic directionality

Keywords : Event Driven Action, Packet Transmission, Traffic Normalization

I. INTRODUCTION

Wireless communications are vulnerable to eavesdropping by anyone equipped with a wireless receiver. When the transmitted information is of sensitive nature, its privacy is protected via cryptographic methods. However, encryption alone cannot prevent the leakage of contextual information such as the location of communicating nodes, the path between the source and the destination, or the time of occurrence of a reported event. Passive eavesdroppers can obtain contextual information by performing traffic analysis using low-level packet identifiers such as packet size and inter-packet timings, even when the contents of the packet remain hidden. Moreover, this information can be used to launch intelligent attacks of selective and adaptive nature that degrade network performance at low cost. In this paper, we address the problem of preserving the privacy of contextual information in wireless communications. Though we study this problem in the context of wireless sensor networks (WSNs), our methods are applicable to any static wireless multi-hop network. We consider an adversary that deploys a network of colluding eavesdroppers at unknown locations within the WSN. The eavesdropping devices can be cheap passive sensors that form an out-of-band collusion network. Eavesdroppers extract communication attributes of interest and centrally process them to derive contextual information. State-of-the art techniques for hiding contextual information employ bogus transmissions to normalize the eavesdropped transmission patterns. In these schemes, sensors transmit according to a predefined distribution, irrespective of their real traffic profile. Transmissions of real packets conform to the same distribution, thus defeating traffic analysis techniques. However, when the locations of the colluding eavesdroppers are unknown, privacy can be achieved only if all sensors become sources of bogus traffic. In our approach, we significantly reduce the communication overhead by intelligently selecting the bogus sources and loosely coordinating real packet transmissions. Our Contributions: We propose a resource-efficient traffic normalization scheme that

protects contextual information under colluding eavesdroppers. Our scheme achieves perfect privacy while the number of bogus traffic sources is reduced. We map the problem of reducing the bogus traffic sources to the problem of partitioning the WSN into minimum connected dominating sets (MCDSs). Due to the problem complexity, we propose a distributed heuristic algorithm that approximates the WSN partition to MCDSs. We further propose a schedule assignment scheme that reduces packet delay by loosely coordinating transmissions among neighbouring sensors. The remainder of the paper is organized as follows.

II. METHODS AND MATERIAL

A. Architecture of system

In this system architecture it will explain about the system is structured to get the detail from various sensors without being intercepted by external resources. The sensor collects information about temperature and sends it to the sink node without being intercepted by any eavesdropper nodes.

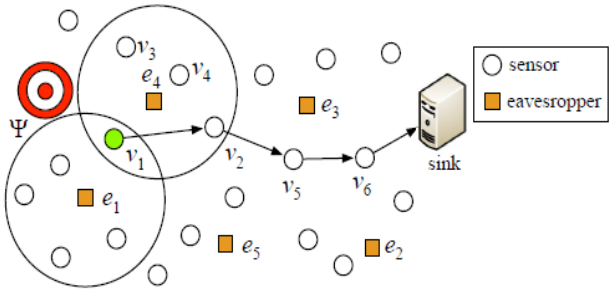

Figure 1. System Architecture

B. Literature Survey

Typical packet traffic in a sensor network reveals pronounced patterns that allow an adversary analyzing packet traffic to deduce the location of a base station. Once discovered, the base station can be destroyed, rendering the entire sensor network inoperative, since a base station is a central point of data collection and hence failure. This paper investigates a suite of de-correlation countermeasures aimed at disguising the location of a base station against traffic analysis attacks. A set of basic countermeasures is described, including hop-by-hop re-encryption of the packet to change its appearance, imposition of a uniform packet sending rate, and removal of correlation between a packet's receipt time and its forwarding time.

- Once discovered, the base station can be destroyed, rendering the entire sensor network inoperative, since a base station is a central point of data collection and hence failure.
- This paper investigates a suite of de-correlation countermeasures aimed at disguising the location of a base station against traffic analysis attacks.
- In habitat monitoring applications, when a sensor node detects an endangered animal, e.g., a panda, it reports the animal's presence and activities to the sink.
- However, the adversaries can eavesdrop on the network transmissions and make use of the traffic information to locate pandas to hunt them.
- Hotspot phenomenon is defined then we develop a realistic adversary model assumption.

C. System Development

System Construction: We consider a set of sensors ***v,*** deployed to sense physical events within a given area. When a sensor detects an event of interest, it sends a report to the sink via a single-hop or a multi-hop route (depending on the relative sensor-sink position). The confidentiality of the report is protected using standard cryptographic methods. Packet transmissions are re-encrypted on a per-hop basis to prevent tracing of relayed packets. Sensors are aware of their one- and two-hop neighbors by using a neighbor discovery service. The sensor communication areas could be heterogeneous and follow any model. The WSN is loosely synchronized to a common time reference. The maximum network-wide synchronization error is □t. Finally, the wireless medium is assumed to be lossy.

Traffic Analysis: This Module, we propose a general traffic analysis method for inferring contextual information. Our method is meant as a baseline for evaluating the performance of protection mechanisms with varying underlying assumptions. Therefore, it relies on minimal information, namely the packet interception times and eavesdroppers' locations. Our method is agnostic to the network topology (though it is inferred) and to the specific mechanism used to counter traffic analysis, so that it can be broadly applied. We emphasize that our goal is not to create the most sophisticated attack. Such an attack is highly-dependent on the protection mechanism and may require additional a priori knowledge. Our method proceeds in the two stages: a traffic cleansing stage followed by a contextual information inference stage.

*Traffic Normalization:*To counter traffic analysis, most existing solutions introduce bogus traffic at every sensor. This is because all sensors are potential sources and the eavesdroppers' locations are unknown. Moreover, the normalized traffic patterns can lead to the accumulation of packet delay on a per-hop basis. For instance, consider the path *p(s, d).* Assume that the traffic rate of every sensor is normalized to one packet per *T*. The worst-case forwarding delay is equal to | *p(s, d)* | *T*, where | *p(s, d)* | is the path length in hops. This delay occurs when downstream sensors transmit earlier than upstream ones within each interval. In the best case, the forwarding delay reduces to *T*, when upstream sensors transmit earlier than downstream.

*Source Location Privacy:*To report **Ψ**, sensor *v* replaces dummy packets with real ones, while maintaining its transmission schedule. Note that real packets are indistinguishable from dummy ones due to the application of per-hop packet re-encryption. Downstream sensors receiving *v*'s report continue to forward it by substituting dummy packets with real ones. By applying Tag Cleansing, the eavesdropper can reduce the locations of the dummy transmissions to location approximation areas of the sensors in *Di*. However, events cannot be meaningfully distinguished by the application of Event Filtering. Moreover, the set of candidate sources cannot be reduced below the set of sensors in *Di.*

III. RESULT

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

IV.CONCLUSION

The result of the project is described from the perspective of the aim and scope set in the beginning of the thesis. We addressed the problem of contextual information privacy in WSNs under a global eavesdropper. We presented a general traffic analysis method for collectively processing the packet interception times and eavesdropper locations at a fusion center. The method is agnostic to the protection mechanism and can be used as a baseline for evaluating different schemes. To mitigate global eavesdropping, we proposed traffic normalization methods that regulate the sensor traffic patterns of a subset of sensors that form MCDSs. We developed two algorithms for partitioning the WSN to MCDSs and SS-MCDSs and evaluated their performance via simulations. Compared to prior methods capable of protecting against a global eavesdropper, we showed that limiting the dummy traffic transmissions to MCDS nodes, reduces the communication overhead due to traffic normalization. We further proposed a loose transmission coordination scheme that reduces the end-to-end delay for reporting events.

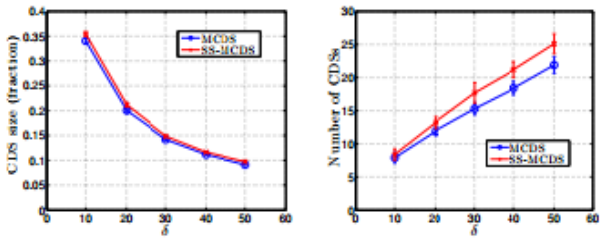

Figure 2. Average CDS size normalization and Average number of CDS

V. REFERENCES

[1] Alejandro Proañ o, Loukas Lazos, and Marwan Krunz : Traffic decorrelation techniques for countering a global eavesdropper in wsn. 2016. IEEE Transactions on Mobile Computing.

[2] M. Akhlaq and T. R. Sheltami. RTSP: An accurate and energy-efficient protocol for clock synchronization in wsns. IEEE Trans- actions on Instrumentation and Measurement, 62(3):578–589, 2013.

[3] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran. Toward a statistical framework for source anonymity in sensor networks. IEEE Transactions on Mobile Computing, 12(2):248–260, 2013.