IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 26-29

Traffic Decorrelation Techniques For Countering A Global Eavesdropper In Wsns

[1]R.Sindhuja,S.Subasri, M.Thilagavathi, UG Student,
[2]Mrs.K.subha,Assistant Professor.
[1](Dept of Computer Science and Engineering, Surya Group of institution, vikravandi)
[2](Dept of Computer Science and Engineering, Surya Group of institution, vikravandi)
Corresponding author: R.Sindhuja

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.*

I. Introduction

TheWireless sensor networks (WSNs) have shown great potential in revolutionizing many applications including military surveillance, patient monitoring, agriculture and industrial monitoring, smart buildings, cities, and smart infrastructures. Several of these applications involve the communication of sensitive information that must be protected from unauthorized parties. As an example, consider a military surveillance WSN, deployed to detect physical intrusions in a restricted area [21], [25]. Such a WSN operates as an event-driven network, whereby detection of a physical event (e.g., enemy intrusion) triggers the transmission of a report to a sink.

Although the WSN communications could be secured via standard cryptographic methods, the communication patterns alone leak contextual information, which refers to event-related parameters that are inferred without accessing the report contents. Event parameters of interest include: (a) the event location, (b) the occurrence time of the event, (c) the sink location, and (d) the path from the source to the sink [10], [20], [23], [29]. Leakage of contextual information poses a serious threat to the WSN mission and operation. In the military surveillance scenario, the adversary can link the events detected by the WSN to compromised assets. Moreover, he could correlate the sink location with the location of a command center, a team leader, or the gateway. Destroying the area around the sink could have far more detrimental impact than targeting any other area. Similar operational concerns arise in personal applications such as smart homes and body area networks. The WSN communication patterns could be linked to one's activities, whereabouts, medical conditions, and other private information. Contextual information can be exposed by eavesdropping on over-the-air transmissions and obtaining transmission attributes, such as inter-packet times, packet A preliminary version appeared at the ACM WiSec 2013 Conference.

source and destination IDs, and number and sizes of transmitted packets. As an example, consider the detection of event by sensor v1 in Fig. 1. Sensor v1 forwards an event report to the sink via v2, v5, and v6: Transmissions related to this report are intercepted by eavesdroppers e1 □ e5. The event location can be approximated to the sensing area of v1. The latter can be estimated as the interception of the reception areas of e1 and e4, which overhear v1's transmissions. Moreover, the event occurrence time can be approximated to the overhearing time of v1's first transmission.

Defending against eavesdropping poses significant challenges. First, eavesdroppers are passive devices that are hard to detect. Second, the availability of low-cost commodity radio hardware makes it inexpensive to deploy a large number of eavesdroppers. Third, even if encryption is applied to conceal the packet payload, some fields in the packet headers still need to be transmitted in the clear for correct protocol operation (e.g.,

PHY-layer headers used for frame detection, synchronization, etc.). These unencrypted fields facilitate accurate estimation of transmission attributes.

The problem of preserving contextual information privacy has been studied under various adversarial scenarios. Threat models can be classified based on the adversary's network view (local vs. global) or the capabilities of the eavesdropping devices (packet decoding, localization of the transmission source, etc.). Under a local model, eavesdroppers are assumed to intercept only a fraction of the WSN traffic [12], [16]–[20]. Hiding methods include random walks, adding of pseudo-sources and pseudo-destinations [14], [17]–[19], [27], creation of routing loops [12], and flooding [12]. These methods can only provide probabilistic obfuscation guarantees, because eavesdroppers locations are unknown. Under a global model, all communications within the WSN are assumed to be intercepted and collectively analyzed [7], [20], [29]. State-of-the-art countermeasures conceal traffic associated to real events by injecting dummy packets according to a predefined distribution [4], [20], [23], [28]. In these methods, real transmissions take place by substituting scheduled dummy transmissions, which decorrelates the occurrence of an event from the eavesdropped traffic patterns. However, concealment of contextual information comes at the expense of high communication overhead and increased end-to-end delay for reporting events.

Our Contributions: We study the problem of resourceefficient traffic randomization for hiding contextual information

in event-driven WSNs, under a global adversary.Our main contributions are summarized as follows: We present a general traffic analysis method for

inferring contextual information that is used as a baseline for comparing methods with varying assumptions. Our method relies on minimal information, namely packet transmission time and eavesdropping location.

We propose traffic normalization methods that hide the event location, its occurrence time, and the sink location from global eavesdroppers. Compared to existing approaches, our methods reduce the communication and delay overheads by limiting the injected bogus traffic. This is achieved by constructing minimum connected dominating sets (MCDSs) and MCDSs with shortest paths to the sink (SSMCDSs). We characterize the algorithmic complexity for building SS-MCDSs and develop efficient heuristics.

To reduce the forwarding delay, we design a rate control scheme that loosely coordinates sensor transmissions over multi-hop paths without revealing real traffic patterns or the traffic directionality.We compare privacy and overhead of our techniques to prior art and show the savings achieved.

Organization: Section 2 presents related work. In Section 3, we state the system and adversary models. Traffic analysis techniques for extracting contextual information are presented in Section 4. In Section 5, we introduce our mitigation techniques. We evaluate their privacy and performance in Section 6 and conclude in Section.

II. Proposed & Modification System

We study the problem of resource efficient traffic randomization for hiding contextual information in event-driven WSNs, under a global adversary.

Our main contributions are summarized as follows:

We present a general traffic analysis method for inferring contextual information that is used as a baseline for comparing methods with varying assumptions.

Our method relies on minimal information, namely packet transmission time and eavesdropping location.

We propose traffic normalization methods that hide the event location, its occurrence time, and the sink location from global eavesdroppers.

Compared to existing approaches, our methods reduce the communication and delay overheads by limiting the injected bogus traffic. This is achieved by constructing minimum connected dominating sets (MCDSs) and MCDSs with shortest paths to the sink (SSMCDSs).

We characterize the algorithmic complexity for building SS-MCDSs and develop efficient heuristics.

To reduce the forwarding delay, we design a rate control scheme that loosely coordinates sensor transmissions over multi-hop paths without revealing real traffic patterns or the traffic directionality**.**

III. Algorithm

Event Filtering-algorithm -identifies the number of packets transmitted. Topology Approximation-algorithm -Estimate the number of packets sent by the source to report. Contextual Information Inference-algorithm –sensor event, location, occurrence time, path, sink location is estimated

IV. Architecture Diagram

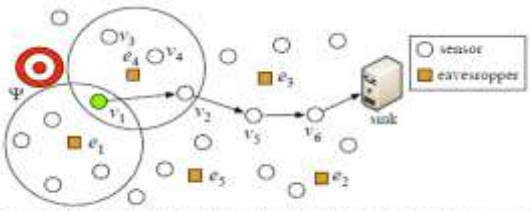

Fig. 1: Detection of event Ψ by eavesdroppers $e_1 - e_5$.

V. Dataflow Diagram

VI. Modules

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:

In 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.

VII. Conclusion

A Source-location privacy is critical to the successful deployment of wireless sensor networks. In this paper, we first propose and analyze a routing-based scheme through single-intermediate node. Then two multi-intermediate nodes schemes are introduced. For each of these schemes, we carried out simulations to evaluate the performances. Simulation results demonstrate that the proposed schemes can achieve very good performance in energy consumption, message delivery latency and message delivery ratio.

In this study we analyzed the energy dissipation and network lifetime characteristics ofmethods for preserving event-unobservability in wireless sensor networks through novel LP formulations. Hence, we introduced a systematic methodology of analyzing such mechanisms underwidely accepted network models (e.g., lifetime definition, energy dissipationmodel, and network topologies) [8,9]. Therefore, both the LP framework and the analysis performed by using this framework are novel technical contributions to the literature. We are not aware of any existing work attempted such an analysis. Any service designed for wireless sensor networks (including security services) must adhere to the general expectations fromwireless sensor networks, one ofwhich is energy efficiency and network lifetime optimization. Hence, our study closes the gap between the provided service (proxy filtering service) and the performance metric (network lifetime) through the developed framework (LP model that captures both energy dissipation and proxy filtering).

References

[1] D. Cox, E. Jovanov, and A. Milenkovic, "Time synchronization for ZigBee networks," in Proc. of the Thirty-Seventh Southeastern Symposium, System Theory, pp. 135-138, 2005.

[2] Wireless Medium Access Control (MAC) and Physical Layer Specifications for Low Rate Wireless Personal Area Networks (LRWPANS), IEEE standard for Information Technology-Part 802.15.4- 2003.

[3] Wireless Medium AccessControl (MAC)and Physical Layer (PHY) Specifications for Low–Rate Wireless Personal Area Net2 works (LRWPANs), IEEE Standards 802.15.4TM-2003.

[4] Wireless Medium Access Control (MAC) and Physical Layer(PHY) specifications for low———Rate Wireless Personal Area Networks (LR - WPANs), IEEE 802. 15. 4. W. LI, et al, Introductory and actual combat of Zigbee wireless networks, Beijing University of Aeronautics And Astronautics Press, April 2007. [6] Zigbee Specification, Zigbee Alliance, June, 2005.

[5] J. Shen and L. Hao, Zigbee MCU Principal and Application based on STM32W Radio Frequency, Beijing University of Aeronautics And Astronautics Press, September 2010.

[6] W. Zhang, L. Feng, and Z. Wen, "Research on home networking with Zigbee," Journal of Hefei University of Technology, vol. 28, pp. 755- 759, 2005. [9] Y. Wang and G. Shen, "ZigbeeWireless Sensor Network Technology and Application," Ship Electronic Engineering, 10th ed, vol. 28, pp. 32-34, 2008.

[7] Y. PENG, LI Yingli et al, "Method for Saving Energy in Zigbee Network," WiCom' 09. 5th International Conference on, pp. 1-3, 2009.