IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 8, August 2018

Detect Eavesdropper and Traffic Analysis in Wireless Sensor Network to Measuring Global Warming

Rozina Barveen.K [1] and Dr. S.J.Sathish Aaron Joseph[2]

Asst Professor, Dept of Computer Science, PT M.G.R arts and Science College, Uchupuli, Tamilnadu[1]

Asst Professor and HOD of Computer Application, J J College of Arts and Science, Pudukkottai, Tamilnadu[2]

Abstract: The problem is considered under a global eavesdropper who analyses 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. 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%

Keywords: Wireless Sensor Networks, Sensor Networks, Location Monitoring, eavesdropping.

I. INTRODUCTION

Wireless 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 .Such 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 networking features to latent features for product recommendation. In specific, we propose learning both users' and products' feature representations (called user embedding's and product embedding's, respectively) from data collected from ecommerce websites using recurrent neural networks and then apply a modified gradient boosting trees method to transform users' social networking features into user embedding's. We then develop a feature based matrix factorization approach which can leverage the learnt user embedding's for cold-start product recommendation. 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. In tis Project 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. 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.

II. PROBLEM IDENTIFICATION

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. Hiding methods include random walks, adding of pseudo-sources and pseudo-destinations, creation of routing loops, and flooding.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

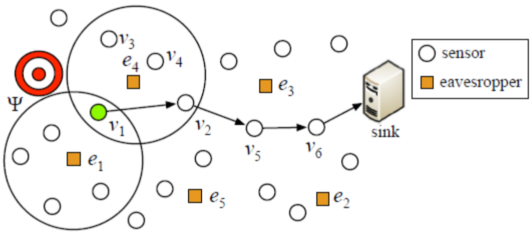
Vol. 7, Issue 8, August 2018

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 analysed.

III. PROPOSED WORK

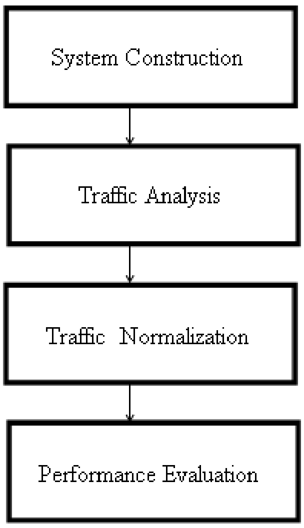
- We study the problem of resource efficient traffic randomization for hiding contextual information in event-driven WSNs, under a global adversary.
- Our main contributions are summarized as follows:
- We present a general traffic analysis method for inferring contextual information that is used as 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.

IV. ARCHITECTURAL DESIGN



The system architecture is the computational design that defines the structure and/or behavior of a system. System architecture is a conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. A system architecture can comprise system components that will work together to implement the overall system.

Our analysis shows that most existing countermeasures either fail to provide adequate protection, or incurhigh communication and delay overheads. To mitigate the impact of eavesdropping, we propose resource-efficient traffic normalizationschemes. In comparison to the state-of-the-art, our methods reduce the communication overhead by more than 50%; and the end-toenddelay 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 theWSN. We further reduce packet delay by loosely coordinating packet relaying, without revealing the traffic directionality.



Each component in a DFD is a labeled with a name. Process names are further identified with a number that will be used does not present the sequence of processed.

V. MODULE EXPLANATION

1. System Construction
2. Traffic Analysis
3. Traffic Normalization
4. Performance evaluation

1. 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

2.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.

3. 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.

4. Performance evaluation

- To analyses the performance to compare the past and present work

Figure 1: Result Node Sensing Node

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 8, August 2018

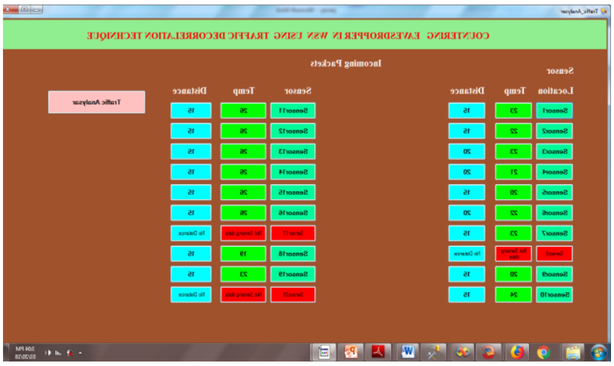


Figure 2 : Result of Counting Eavesdropper

Figure 3 : Finding Eavesdropper

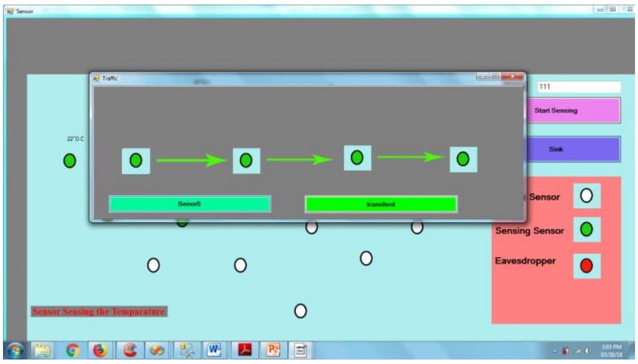


Figure 4: Sensing path

V. CONCLUSION AND FUTURE SCOPE

CONCLUSION

In this paper, we formalize the location privacy issues under the model of a global eavesdropper and show the minimum average communication overhead needed for achieving a given level of privacy. We also presented two techniques to provide privacy against a global eavesdropper. Analysis and simulation studies show that they can effectively and efficiently protect location privacy in sensor networks.

FUTURE SCOPE

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 large number of eavesdroppers.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 8, August 2018

REFERENCES

[1] M. Akhlaq and T. R. Sheltami. RTSP: An accurate and energyefficientprotocol for clock synchronization in wsns. IEEE Transactionson Instrumentation and Measurement, 62(3):578–589, 2013.

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

[3] F. Armknecht, J. Girao, A. Matos, and R. Aguiar. Who said that?privacy at the link layer. In Proc. of the INFOCOM Conference,pages 2521–2525, 2007.

[4] K. Bicakci, H. Gultekin, B. Tavli, and I. Bagci. Maximizing lifetimeof event-unobservable wireless sensor networks. ComputerStandards & Interfaces, 33(4):401–410, 2011.

[5] G. Chinnu and N. Dhinakaran.Protecting location privacy inwireless sensor networks against a local eavesdropper–a survey.International Journal of Computer Applications, 56(5):25–47, 2012.

[6] M. Conti, J. Willemsen, and B. Crispo.Providing source locationprivacy in wireless sensor networks: A survey. CommunicationsSurveys Tutorials, 15(3):1238–1280, 2013.

[8] 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.

[9] 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.

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

[11] 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.

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

[13] 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.

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