International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 4 – APRIL 2018.

# PREVENTION OF EAVESDROPPER ATTACKS USING DECORRELATION PATTERNS IN WIRELESS SENSOR NETWORKS

E. Sivaranjani [#1] and R. Angelin Preethi [*2]

[#] *M.Sc (Computer Science), Department of Computer science, Kamban College of Arts and Science for women, India*

[*] *Assistant Professor, Department of Computer science, Kamban College of Arts and Science for women, India*

**Abstract- Traffic analysis has traditionally been a major threat to wireless tactical military communications. An adversary with the ability to obtain network measures such as packet counts at various links, correlations in sending and receiving times, etc. may deduce sensitive information about existing communication patterns. In this paper, we propose Decorrelation techniques which prevent the activities performed by eavesdropper. In specific to, the global eavesdropper that threatens the sensitive attributes like number of transmitted packets, inter-packet times, and traffic directionality, to infer event location, its occurrence time, and the sink location. The traffic analysis method is been incorporated for finding the correlating patterns of the transmission systems. Based on the contextual information of the eavesdropper, the similar patterns are correlated for efficient transmission systems. Experimental results have shown the efficiency of the proposed algorithm. The proposed system has resolved the issue of high communication cost and delay overhead.**

**Keywords: Traffic analysis, Eavesdropper, Sensitive attributes, Decorrelation and Transmission systems**

## I. INTRODUCTION

Wireless sensor networks (WSNs) have shown tremendous ability in revolutionizing many packages inclusive of military surveillance, patient monitoring, agriculture and business monitoring, smart homes, cities, and smart infrastructures. Numerous of these packages contain the communiqué of sensitive statistics that have to be protected from unauthorized events. As an example, consider a navy surveillance WSN, deployed to hit upon bodily intrusions in a limited area [1]. The sort of WSN operates as an event-pushed network, whereby detection of a bodily event (e.g., enemy intrusion) triggers the transmission of a record to a sink.

Even though the WSN communications may be secured through preferred cryptographic techniques, the conversation patterns on my own leak contextual records, which refer to event-related parameters that are inferred without accessing the record contents. Event parameters of hobby encompass: (a) the occasion area, (b) the prevalence time of the occasion, (c) the sink region, and (d) the path from the source to the sink [2]. Leakage of contextual records poses a extreme chance to the WSN mission and operation. Within the navy surveillance state of affairs, the adversary can hyperlink the events detected with the aid of the WSN to compromised assets. Moreover, he may want to correlate the sink vicinity with the region of a command center, a group chief, or the gateway. Destroying the vicinity around the sink ought to have a ways more damaging impact than targeting some other area. Comparable operational issues arise in non-public applications including smart houses and body place networks. The WSN conversation patterns may be connected to at least one's sports, whereabouts, scientific conditions, and other personal information.

Safeguarding against listening stealthily postures noteworthy difficulties. To start with, busybodies are inactive gadgets that are difficult to recognize. Second, the accessibility of ease ware radio equipment makes it reasonable to de-ploy an expansive number of spies. Third, regardless of the possibility that encryption is connected to cover the parcel payload, a few fields in the bundle headers still should be transmitted free for adjust convention operation (e.g., PHY-layer headers utilized for outline recognition, synchronization, and so forth.). These decoded fields encourage precise estimation of transmission qualities. Latest countermeasures conceal traffic related to actual activities by using injecting dummy packets in step with a predefined distribution [3]. In these methods, actual transmissions take place by means of substituting scheduled dummy transmissions, which decorrelates the incidence of an event from the eavesdropped site visitor's styles. However, concealment of contextual facts comes at the fee

of excessive verbal exchange overhead and multiplied stop-to-quit de-lay for reporting occasions.

The rest of the paper is organized as follows: Section II describes the related work; Section III presents the proposed work; Section IV presents the experimental analysis and finally concludes in Section V.

## II. RELATED WORK

This section presents the prior works available on attacks prevention in Wireless Sensor Networks (WSNs). Previous artwork on contextual information privateness can be classified primarily based on the privacy type and the eavesdropper abilities. Widespread literature critiques can be observed in recent surveys [5], [6]. Right here, we gift related paintings for countering nearby and international eavesdroppers. Neighborhood eavesdropper: a local adversary can intercept a restrained range of transmissions in the WSN. Normally, this adversary deploys a single or some cellular devices that try to localize source with the aid of backtracking the intercepted transmissions. In [7], the authors proposed using a couple of routing paths to save you nearby adversaries from tracing packets to their source. A sensor with a real packet for transmission forwards it to 1 neighbor at the shortest path to the sink. Any overhearing sensor that doesn't belong to the shortest path, broadcasts a dummy packet with some probability. This opportunity is customized to maintain the identical common communication overhead according to sensor.

The author in [8] considered a enormously capable adversary that could exactly localize the supply of a transmission using radiometric hardware. They proposed the hotspot-finding attack for figuring out regions with high transmission hobby and analytically confirmed that the supply may be placed thru backtracking. To cover the source vicinity, the authors proposed the creation of dummy traffic from sensor clouds that turn out to be lively only for the duration of real transmissions. In [9], the authors proposed a -stage routing technique called phantom flooding. Inside the first stage, the source divides its associates into units, located in opposite guidelines (e.g., north-south). The supply forwards a packet to a randomly selected neighbor in a single course. This neighbor keeps to forward the packet in the identical way, however in the opposite direction. The process is repeated until h hops are traversed. Inside the 2d degree, the packet is forwarded to the sink the use of probabilistic flooding. The real packets are diverted to a fake source placed numerous hops away, the usage of unicast transmissions. The fake source forwards packets to the sink using flooding or over the shortest path. These works vary in the choice system of the fake source. In megastar, an intermediate node is chosen from a sink toroidal place. This region forms a ring around the sink, beginning from radius r and ending at r. to report an event, the supply routes packets to a random destination in the toroidal place. The intermediate faux source relays the packet to the sink via the shortest course.

To lessen the stop-to-end put off, sensors with real packets “rush” their transmissions relative to scheduled dummy transmissions. Future dummy transmissions are not on time to atone for the rushed real packets. This method is not effective while multiple actual packets should be transmitted via the equal source. Similarly, the authors in [10] proved that the quick-long inter-packet time styles discovered due to the rushed transmissions can be used to become aware of time periods that incorporate real packets. To deal with this vulnerability, they delivered faux quick-lengthy styles. Several methods for reducing dummy site visitors were suggested. The community becomes divided into rectangular cells of size same to the minimal place unit in which occasions can arise. Each cellular generates encrypted bogus traffic, that's changed with actual traffic while to be had. Inside the proxy-primarily based filtering scheme (PFS), a sub-set of cells are special as proxies. Every cellular transmits packets (real or dummy) to the closest proxy, which filters dummy site visitors and forwards real packets to the sink. The WSN is split into clusters, each with one cluster head (ch). The chs are prepared in a tree rooted on the sink. Every sensor transmits dummy visitors to its respective ch. The ch is liable for filtering dummy packets, aggregating real packets, and relaying them to the sink. This method does now not conceal the sink location, which corresponds to the foundation of the ch tree.

## III. PROPOSED WORK

This section presents the proposed model of the domain study. The main objectives of the proposed study are:

- To study the problem of resource efficient traffic randomization for hiding contextual information in event-driven WSNs, under a global adversary.
- To propose traffic normalization methods that hides the event location, its occurrence time, and the sink location from global eavesdroppers.
- 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.

The proposed model composes of four phases, namely,

### *A) Construction of Network system*

Let us consider a set of sensors $s_i$ deployed in certain sensing 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 Δt. Finally, the wireless medium is assumed to be lossy.

*B) Analysis of Traffic:*

A general traffic analysis method for inferring contextual information is designed. 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. It 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. It also emphasizes 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 precedes in the two stages i.e a traffic cleansing stage followed by a contextual information inference stage.

*C) Privacy for source location:*

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*.

By doing so, we have achieved the following merits:

- The proposed system reduces the communication and delay overheads by limiting the injected bogus traffic.
- The proposed system reduces the forwarding delay
- Significantly, reduced the privacy and overhead of our techniques to prior art and show the savings achieved.

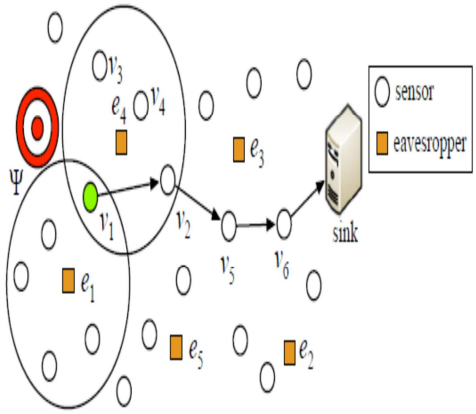


Fig.3.1 Proposed architecture

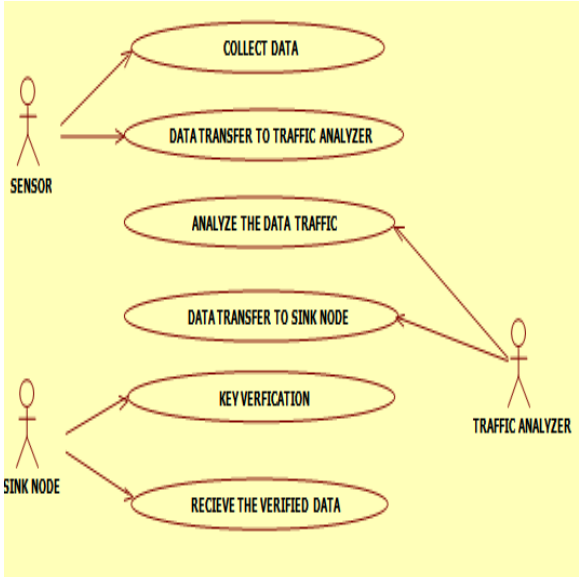


Fig.3.2 Proposed workflow

## IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental analysis of proposed design in DOTNET framework.

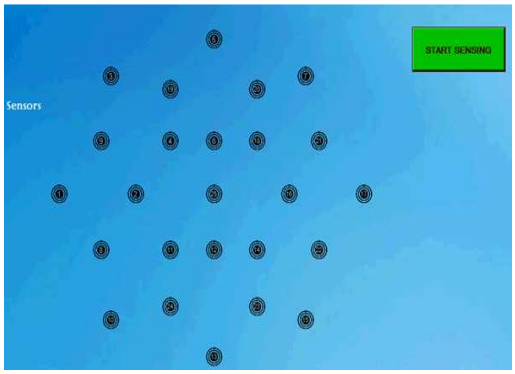


Fig.4.1 Sensing the source and destination nodes


Fig.4.2 Traffic analysis of the packets

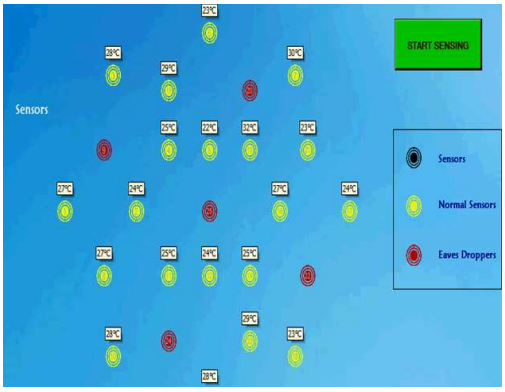


Fig.4.3 Sensors sensing the temperature for file transmission systems


Fig.4.4 Entering the verification keys


Fig. 4.5 Verification of the keys


Fig.4.6 Message validation process

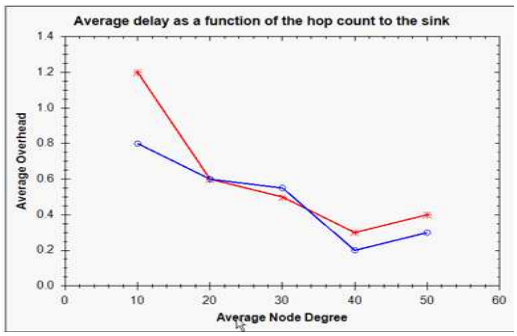


Fig.4.7 Overhead analysis

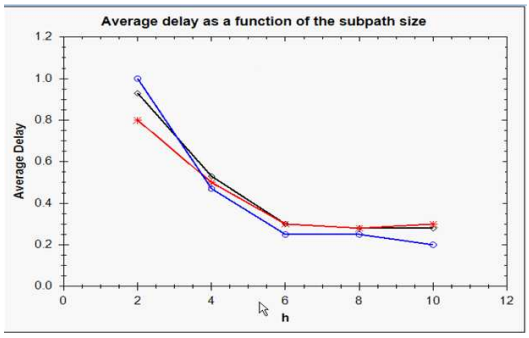


Fig.4.8 Delay analysis

## V. CONCLUSION

Location privacy in sensor networks poses new challenges due to the limitations of sensor nodes regarding computational power, limited communication range, and, more importantly, a modest and non-rechargeable battery supply. Therefore, privacy preservation techniques must trade-off between an appropriate privacy protection level and the cost of applying countermeasures against traffic analysis attacks. Obviously, the more powerful the attacker is, the more resources the network must spend in order to cope with the threat of a privacy breach. In general, the solutions to protect, either source or receiver location privacy, against a local adversary are based on routing protocols which randomize and balance network traffic. In this paper, we propose a Decorrelation technique which prevents the activities performed by the eavesdropper. Once the packet is available for transmission systems, the sensitive attributes like number of transmitted packets, inter-packet times, and traffic directionality, to infer event location, its occurrence time, and the sink location were analyzed. Based on the contextual information of the packets, the correlating patterns are found and thus the eavesdropping is prevented. Experimental results have shown the efficiency of the system.

## REFERENCES

[1] Alejandro Proano et al, “Traffic Decorrelation Techniques for Countering a Global Eavesdropper in WSNs”, IEEE Transactions on Mobile Computing, 2016.

[2] 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.

[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 life-time of event-unobservable wireless sensor networks. Computer Standards & Interfaces, 33(4):401–410, 2011

[5] G. Chinnu and N. Dhinakaran. Protecting location privacy in wireless 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 location privacy in wireless sensor networks: A survey. Communications Surveys Tutorials, 15(3):1238–1280, 2013.

[7] J. Deng, R. Han, and S. Mishra. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. Pervasive and Mobile Computing, 2(2):159–186, 2006.

[8] M. Fruth. Probabilistic model checking of contention resolution in the IEEE 802.15.4 lowrate wireless personal area network protocol. In Proc. of the Symp. on Leveraging Applications of Formal Methods, Verification and Validation, pages 290–297, 2006.

[9] A. Jhumka, M. Leeke, and S. Shrestha. On the use of fake sources for source location privacy: Trade-offs between energy and privacy. The Computer Journal, 54(6):860–874, 2011.

[10] L. Jia, R. Rajaraman, and T. Suel. An efficient distributed algorithm for constructing small dominating sets. Distributed Computing, 15(4):193–205, 2002.