ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

# Phantom Flooding Traffic Detection Techniques for Packet Dropping Centers in WSN

[1] D J Samatha Naidu, [2]C.Sasidhar , [3]N.Reshma Chandrika
[1] Assistant Professor, MCA Department,APGCCS ,[2]Assistant Professor, ,AITS, Rajampet,
[3] vice principal, balaji institute of IT and Management college, kadapa

**Abstract: In broad-spectrum Traffic analysis method used for collectively processing the packet transmitted times and eavesdropping per locations at a fusion center . In Existing work, Treat models can be generalized based on the adversary's network view, the ability of the eavesdropping devices like (packet decoding , localization of transmission).It includes random walks , adding of pseudorandom sources and destinations , flooding etc. In proposed work: Resource oriented efficient traffic normalization schemes are used for comparative study to the state of the art to reduce the communication overhead by more than 50%. End to end packet delay by more than 30% by using round-robin fusion method. This method allows us to reduce the number of traffic source active at a given time while providing routing paths any node in the WSN. It reduce packet end to end delay by loosely coupling coordinating packet relaying, without rerouting the traffic directionality phantom flooding traffic detection done in two stage routing. Here it eliminates hotspot locating attack to identify regions.**

**Index Terms - Introduction, motivational Work, general traffic analysis method, Results**

## 1. INTRODUCTION

Wireless sensor networks (WSNs) have shown great potential in radical change in many applications including military related, health monitoring, agro based and industry related monitoring. Generally wireless sensor networks involves many application to communicate sensitive based information that must be protected from unauthorized access parties. Some cryptographic methods can be used for security related contextual information can be protected which leads towards to event related points can be used without accessing report content information.

***Motivation work***

The parametric analysis shows that most interesting existing related counter measures either fail to provide adequate protection, or incur high communication mode and end to end delay routing overheads. To moderate the impact of eavesdropping, we proposed resource based efficient traffic normalization schemes. In comparative study the state-of-the-art, our proposed methods can be reduced the communication routing overhead by more than 50%; and the end-to-end packet delay by more than 30%. To do so, we entire network can be partition the WSN and connected with minimum dominating sets that allows us to operate in a round-robin fashion. This can be reduce the number of traffic related sources which are act active at a given time, while selecting routing paths to any node in the WSN..

## II. EXISTING WORK – LIMITATIONS

The most challenging research issue of preserving local contextual information security with proposed adversary models. Threat methodologies can be classified based on the adversary's network view (homogenous vs. heterogeneous) or the capabilities of the eavesdropping devices (packet decoding, localization of the transmission source, etc.). Under a homogenous model, eavesdroppers are assumed to interrupt only a portion of the WSN traffic. defeat methods include random walks, adding of pseudo-sink nodes and pseudo-target nodes, creation of routing loops, and data flooding.

***DISADVANTAGES***

- First, eavesdroppers they listen to a conversation without the authencation type of passive devices that are very difficult to detect.
- Second, its very difficult to deploy a large number of eavesdroppers to communicate because of low-cost commodity radio hardware.
- Third, need advanced encryption based techniques to avoid the packet headers still need to correct the protocol related information..

## III. PROPOSED WORK – ADVANTAGES

The proposed work had focuses on various resource efficient traffic related randomization techniques to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

explore the contextual information in event-driven Wireless sensor networks which accept under wide range adversary model.

***The main contributions are summarized as follows:***

- first, apply the base line comparison methods with various assumptions which should follows common traffic analysis methods for intercept contextual information.
- The Proposed method depend on minimum information related details like packet transmission time, arrival time, and source level eavesdropping location. Privacy preserving based locations.
- The proposed relay based traffic normalization methods that hide the event location, its arrival time, and dispatch time , the sink location from large-scale eavesdroppers.
- Compared with all existing approaches, the results shows reduced communication overhead delays by limiting the duplicate path links traffics. This is achieved by constructing minimum connected dominating sets (with shortest paths to the sink.

***Advantages***

- The proposed approach reduces the communication overhead delays by limiting the backup link paths in traffic.
- The proposed approach reduces the forwarding packet delay in between network to network routers.
- We comparative study results shows the optimal results towards eavesdropping.

## IV. PROPOSED WORKING METHODS

***a) System Construction***

We consider a group of sensors called as v, deployed to sense physical events within a given area. When a sensor detects and maintains the report related to the sink via single route hop or a multi-route hop (depending on the relative sensor-sink position). The privacy related report is protected using symmetric cryptographic methods. Packet transmissions over the channels are re-encrypted based on situations which can be aware of sensors during transmission period of time. The sensor now communicates with global transaction which provide maximum utilization of network synchronization based on reference. Finally, the wireless medium is assumed to be lossless.

***b) Traffic Analysis***

In this Module, we proposed relay based traffic generalization analysis method for intercepting contextual information. Which evaluates the performance of privacy mechanisms with varying assumptions. Where packet having long lasting network topology along with some specific network counter traffic analysis related specific mechanism are identified with sophisticated attacks. Such methods yields us in two different stages 1. Traffic can cleansed stage 2. Which followed by a contextual information inference stage.

***C) Traffic Normalization***

The new proposed counter traffic analysis methods identified, most existing solutions introduce back up repeated links in traffic at every sensor network. Moreover, the normalized traffic patterns can lead to the total accumulation period of a end to end packet delay on a each single-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 of packet 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 packet forwarding delay reduces to T, when upstream sensors transmits before downstream.

***D)Source Location Privacy***

To report Ψ, sensor node v replaces with duplicate set of packets along with original one while maintaining the transmission report schedule. When a node suspects any damage or unauthorized movements related to the network node then immediately duplicate copy of encrypted packets can be injected in network. After problem over hides then re-encrypt the original copy of the packets by applying symmetric cryptographic packet transmission in the schedules .By applying this proposed techniques it prevents eavesdropper, which can reduce the preserve based 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 group of candidate sources cannot be reduced below the set of sensors in Di.

***We focuses in evaluating the privacy maintained*** under the analysis of O(W ). We quantify this privacy as the distance between the contingent location based on O(W ) and the location of the source. We call this measure privacy distance and formally define it as follows. Definition 3 (Privacy Distance): Let ∈ Rn be some private information

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

of interest, estimated as Ξ ∈ Rn based on eavesdropping. The privacy distance of ithe adversary uses duplicate tags in the observation set O to obtain a better estimation of transmission set Θ. In Algorithm 1, we present a process for where s(ξ) is the Euclidean distance between and ξ ∈ Ξ, and P (ξ) a probability measure over the points in Ξ. We note that Euclidean distance is a natural measure for evaluating location privacy as it yields the straight- line distance between the source location and its estimate in any dimensional space. As an example, , Ξ ∈ R2 for when location privacy is measured and sensors are deployed in two dimensions. For the WSN sensor node v1 reports the frequent occurrence of event Ψ during each W by its tags to identify various sensors and eliminates duplicate tags. Specifically, for two eavesdroppers a and e with overlapping reception areas, we divide their respective observation sets to tags intercepted in Ca ∩ Ce, Ca\Ce, and Ce\Ca. Each tag set is allied with a sensor label that represents the transmissions within the respective area. The location of each sensor label is approximated by the area intersection (difference) between Ca and Ce. Details are described in Algorithm 1.transmitting Θv1 (W ) to the sink. Eavesdroppers e1 an capture Oe1 (W ) and Oe4 (W ) respectively. By jointly analyzing the collected observation sets, the . adversary.

## RESULTS

The following software and Hardware requirements can be used to develop this paper.

***Software Requirements***

Operating system : Windows 7
Coding Language : .NET,C#
Tool :Visual Studio 2008

***Hardware Requirements***

System : Core2Duo
Hard Disk : 120 GB
RAM : 1GB

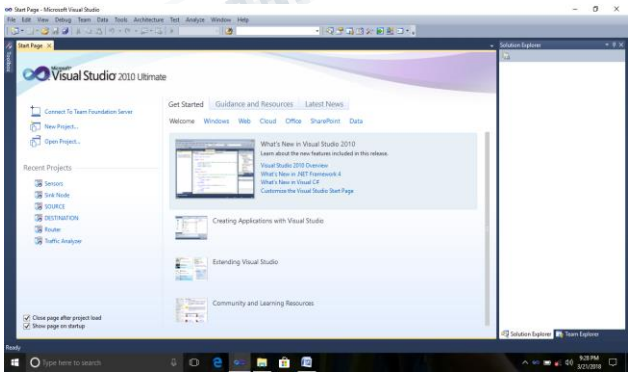



***Fig 1. Microsoft visual studio installation***

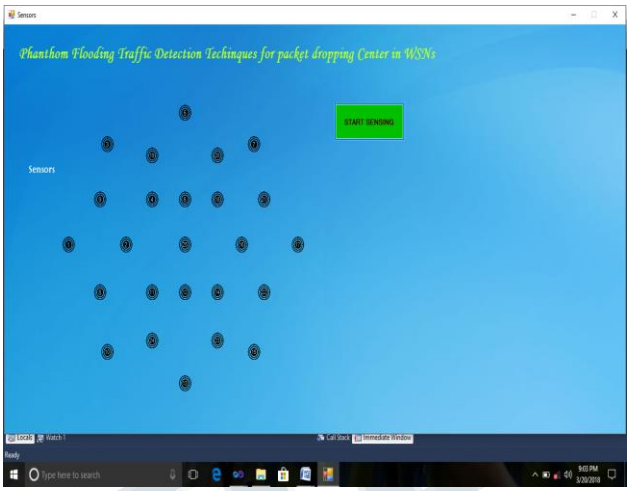
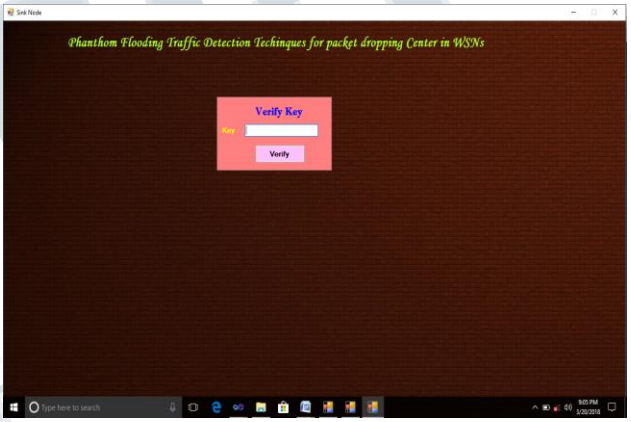
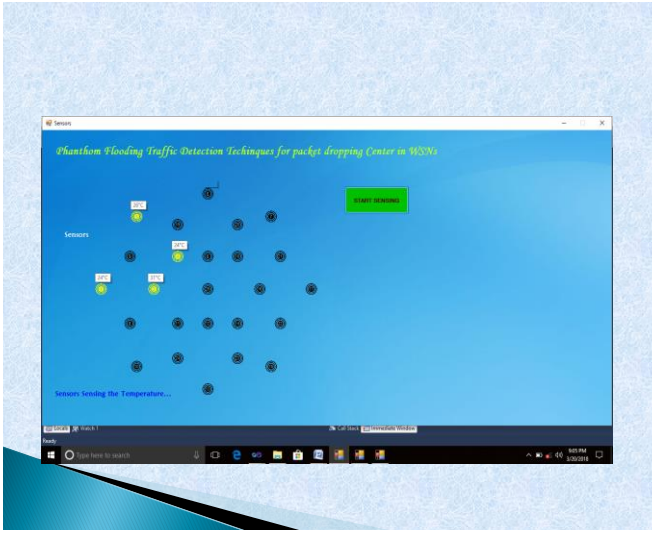



***Fig 2 Node initialization***



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

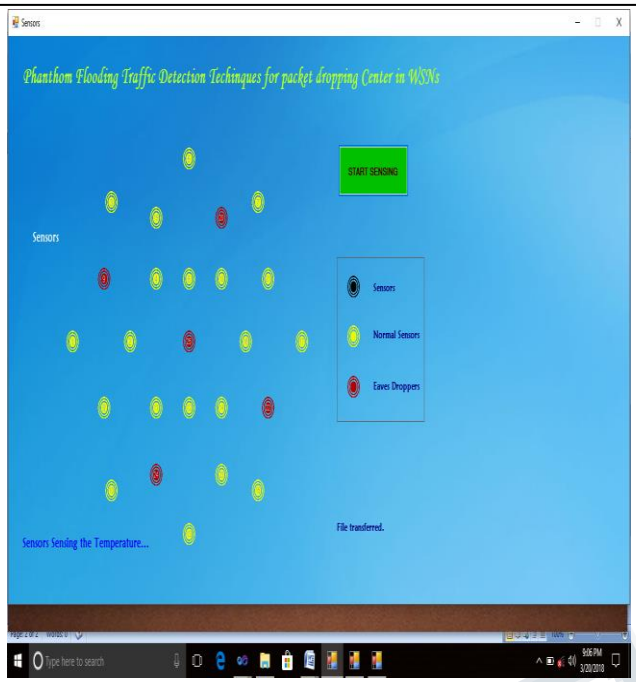



*Fig 3 a) verify the security code for authentication*
*3 b) Packet transmission between nodes.*
*3 c) packet droppers information*

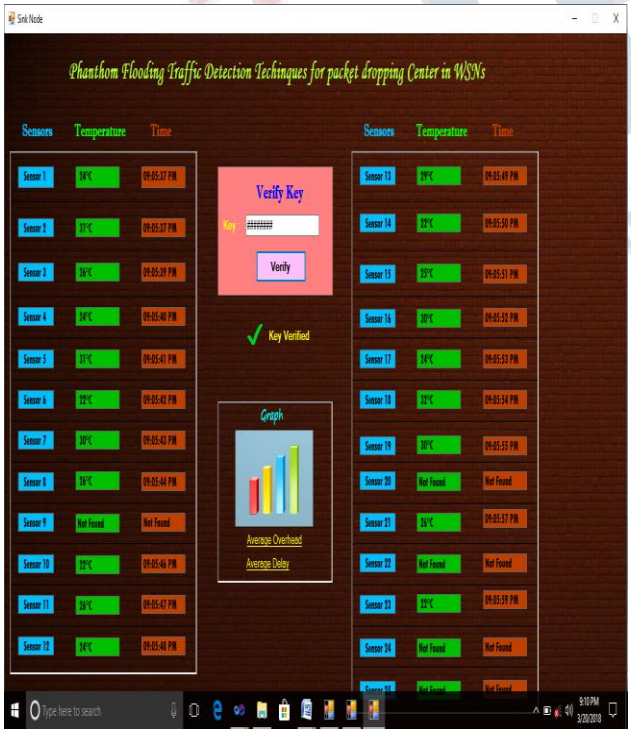



*Fig 4: packet delivery at destination side.*

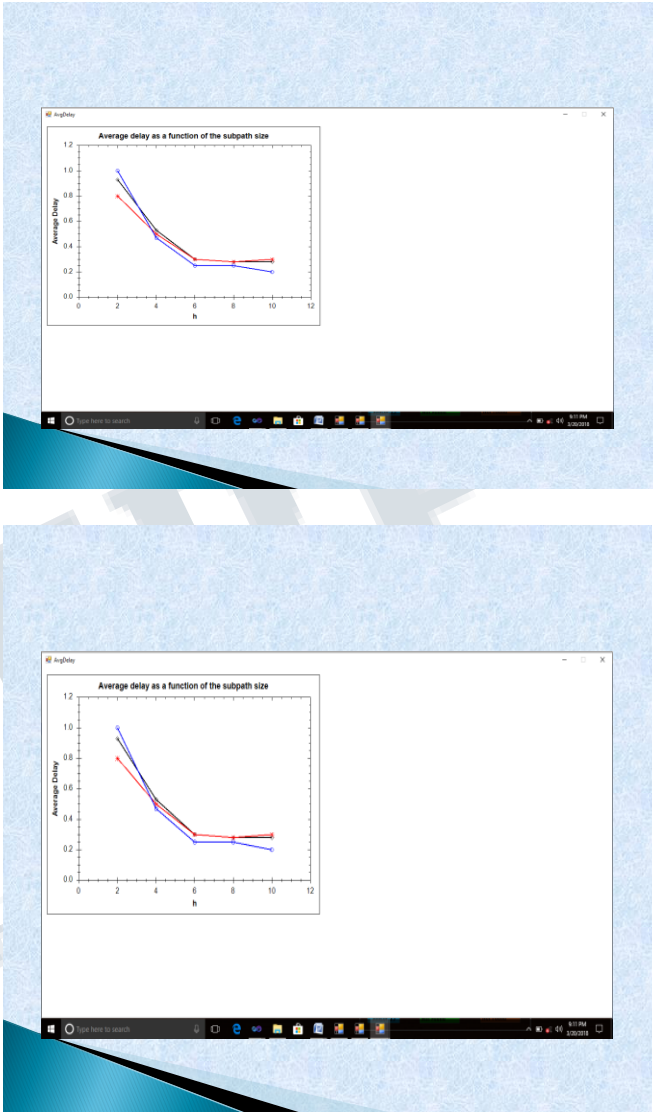



*Fig 5: a) and b) throughput variations during transmission*

## VI CONCLUSION

Finally I conclude that in this paper addressed the problem of contextual information privacy in WSNs under a global eavesdropper. New proposed two algorithms for partitioning the WSN to MCDSs and SS-MCDSs and evaluated their performance via simulations. It showed that limiting the dummy traffic transmissions to MCDS nodes, reduces the communication overhead due to traffic normalization It further proposed a loose transmission coordination scheme that reduces the end-to-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

end delay for reporting events. It is difficult to develop a system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future work that can be done to this system are better to implement to send the file by selecting with user and send the secret using crypto system algorithms.

## REFERENCES

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

[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, 2017.

[4] K. Bicakci, H. Gultekin, B. Tavli, and I. Bagci. Maximizing lifetime 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, 2016.

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

[9] J. Gross and J. Yellen. Handbook of Graph Theory. CRC, 2004. [12] 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, 2012.