Detecting And Monitoring Wormhole in IoT enabled WSNs Using EyeSim

Nilima Nikam, Poorna R. Pimpale, Pranali Pawar, Anita Shirture

Abstract— **The advancement in networking has led to IOT i.e. Internet Of Things. IOT has enabled the communications between the machines i.e. to transfer the data over network without any human intervention. A Wireless Sensor Networks(WSN) which comprises of various node and actuators are integrated with IOT so as to collaborate dynamically with the internet. This paper focuses on the WSNs which are IP enabled and also reviews the tool which is capable of not only detecting but also monitoring the malicious nodes that leads to wormhole attack on the mobile phones.**

Index Terms— **Network Model, Wormhole attack model, system architecture.**

I. INTRODUCTION

The most important content or ingredient for IoT platform is Wireless Sensor Network. The emerging trend of IoT has led to various smart proposals in integration with Wireless Sensor Networks to support smart phones, smart homes, smart workplace. The emerging trends in IP enabled WSNs serves the promising framework but the security challenge remains. In this paper the science of visual analytics is used that facilitates the interactive visual interfaces. The proposed tool EyeSim is based on routing which is dynamic in nature and it also analyses the cognitive network. It detects and monitors the wormholes in the network of the cell phones. The main benefit for visualization is the human perception, intuition and background knowledge. There are many ways in which the events that occur inside the network are represented, and one of them is visualization. It is said that visual representation is anytime better than text representation. Picture carries enormous amount of information like shapes, sizes, colors of different data sets. it was a need to develop a visualization system on mobile system as WSNs are used everywhere.

II. LITERATURE SURVEY

The paper[4] proposed the sensor anomaly visualization engine(SAVE) which represents the fault diagnosis through visualization and it also encompasses the three distinct visualization components that is topological, co-relational and dimensional sensor data dynamics and their anomalies. The paper[10] proposed the visualization system SecVizer which was capable of parsing the generated traffic which was traced from both wired and wireless networks. To obtain the effective detection of the vulnerabilities in the network it combines the visualization topology with the parallel coordinate plot.

III. EXISTING SYSTEM

Visual based anomaly detection system i.e. VisIoT is a human interactive system which is very much capable of monitoring and also detecting various security attacks like Sybil attack or wormhole attacks. This approach proves to be quite effective to find out activities that prove to be malicious like DOS attacks, wormhole attacks but these solutions do not prove to be effective in WSNs.

VisIoT detects the centralized attacks. It uses Intrusion System which is visually assisted for detecting the patterns of the sensor networks in the network. The basic problem is this system discovers the attack but it cant detect the exact location of the attack. this system can only visualize the attacks.

IV. PROPOSED SYSTEM

Thee proposed tool can find out the attacks and threats that occur in the sensor networks which are IP enabled visually.

A. Network Model

- There are N sensor nodes in a deployment area of E metrics which is monitored by EyeSim.
- The exact co-ordinates and the location of the nodes is unknown.
- The radio transmission range of radius R is fixed for each node in the area.
- A sensing coverage of disk equal to R2 quadratic metric units is formed by each node.
- The nodes do not have a fixed pattern to move and they have the speed of S metric units per second.

B. Wormhole Attack Model

- In this attack confusion is created between routing mechanism as nodes fake a route which is shorter than the existing one in the network.
- There is a tunnel of malicious nodes.
- Attack is launched by capturing the packets from one location and transmitting it to distant node.
- As nodes are not aware of their actual location there is no trust model.
- When the attack is launched a link of malicious nodes is formed.
- A low link metric attracts the traffic which is originated by its neighbors.
- The next hop of the node is other edge of wormhole link, actually they are not the neighbors but the malicious nodes.
- Wormhole links move like any other legitimate nodes.

V. SYSTEM ARCHITECTURE

The architecture consists of four modules which is responsible for its network behavior. The four parts are: a)

Nilima Nikam, Professor, CMPN, Y.T.I.E.T, Bhivpuri, Karjat, India
Poorna R. Pimpale, PG Students, CMPN, Y.T.I.E.T, Bhivpuri, Karjat, India
Pranali Pawar, PG Students, CMPN, Y.T.I.E.T, Bhivpuri, Karjat, India
Anita Shirture, PG Students, CMPN, Y.T.I.E.T, Bhivpuri, Karjat, India.

Mobile Client, b)Web Page, c)Server, d)Google Cloud Messenger, e)WSN Topologies.

a)Mobile Client: Application written in JAVA

b)Web Page: Its basically a PHP framework a CodeIgniter.

c)Server:It contains the set of scripts required to find the positions of nodes in the network. the Mobikle Client and the Web site processes the network data using MySQL database which stores the information of all the nodes.

d)Google Cloud Messenger:It baasically allows the system to generate the notifications in the mobile devices. .

e)WSN Topologies:It provides the required topologies to access the wireless sensor networks.

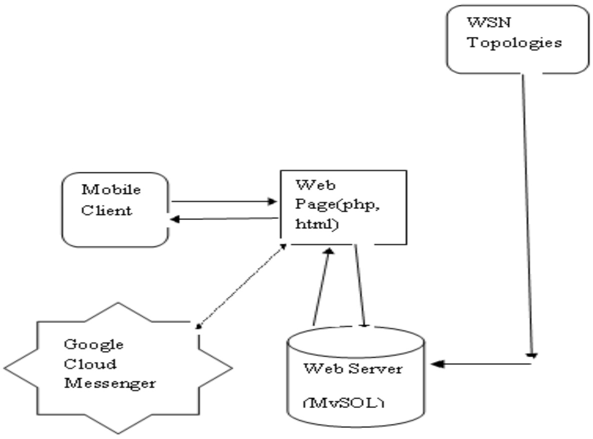


Fig .1. System Architecture

VI. Methodology

EyeSim is the mobile application that guides the user to quickly detect the wormhole attack in IP enabled WSNs.

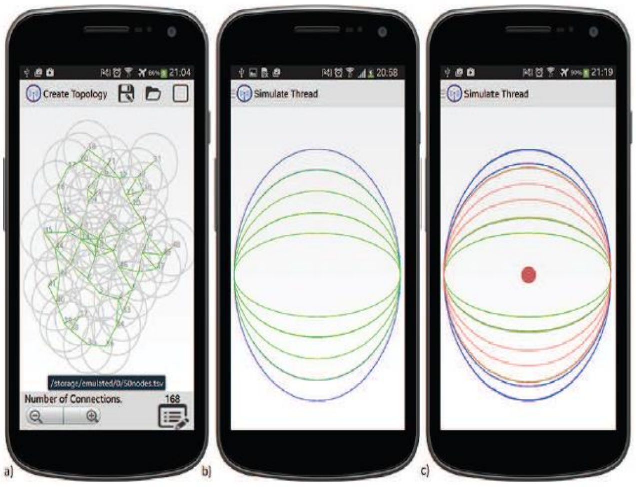


Fig.2. EyeSim GUI

The GUI shows the deployed nodes. Second figure shows the nodes that do not fall in danger zone. Third figure shows the nodes that are marked red which symbolises the attack.

The Eyesim tool is based on two components

1.Engine to detect Wormhole

2.The Visualisation Engine

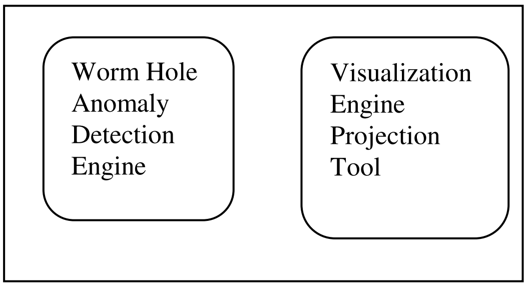

Worm Hole Anomaly Detection Engine
Visualization Engine Projection Tool

Fig.3. Core Components

1.The Wormhole Anomaly Detection Engine: It monitors, detects, and isolates the wormhole attacks in mobile WSNs which do not have authentication entity in common. It analyses the patterns in the network routing dynamics using a cognitive wormhole detection algorithm.

The Algorithm to Detect Wormhole In the Network

Input: Number of Sensor nodes N, time Period T, Neighbour list of all nodes in the network M1,M2,...,MN, routing path of all the nodes in the network R1,R2,...RN, next hoplist of the nodes in the network H1,H2,...,HN.

Output: List of malicious nodes which are detected(W1,W2,...)

```
For each time period T do
Form the U list
$W = R_{U1} \cap R_{U2} \cap \ldots$
$W = W \cap H_{W1} \cap H_{W2} \ldots$
if $W \neq$ then:
Trigger an alarm
Isolate the nodes that are included in W
[End if]
[End for]
```

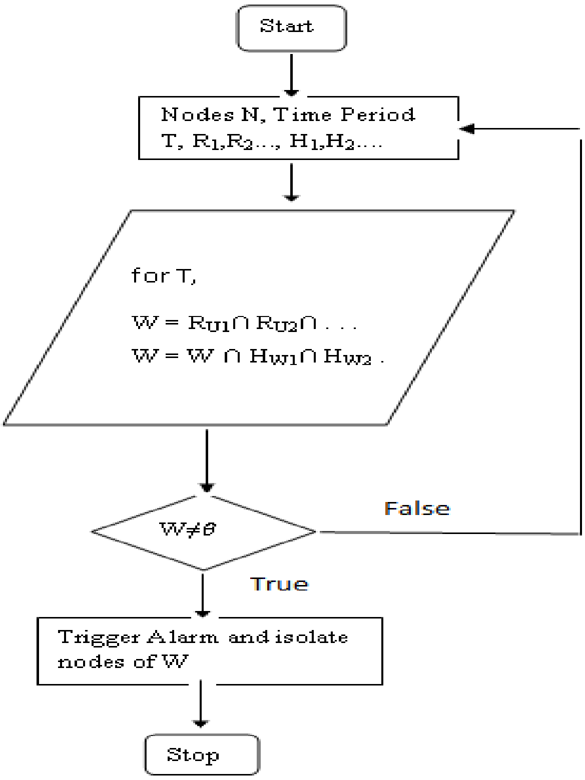
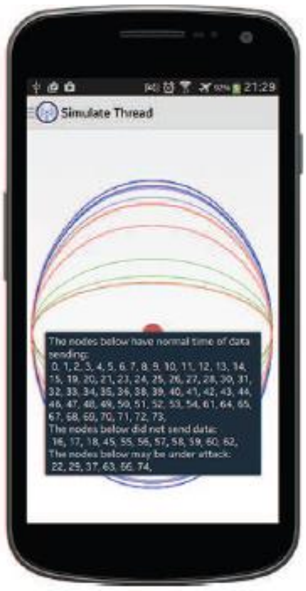

Start
Nodes N, Time Period T, R1,R2..., H1,H2....
for T,
W = RU1∩ RU2∩ . . .
W = W ∩ HW1∩ HW2 .
W≠θ
False
True
Trigger Alarm and isolate nodes of W
Stop

Fig.4. Algorithm for Wormhole Detection

The Visualisation Engine

The objective is to show or project the outcome of the wormhole anomaly detection model in a proper visual way.
1. It should produce effective visualisation interface.
2. The visuals which are projected must be in the form of correct , real time and shoul be able to indicate the threats in the smart phones.



The nodes below have normal time of data sending:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 19, 20, 21, 23, 24, 25, 26, 27, 28, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 50, 51, 52, 53, 54, 61, 64, 65, 67, 68, 69, 70, 71, 72, 73,
The nodes below did not send data:
16, 17, 18, 45, 55, 56, 57, 58, 59, 60, 62,
The nodes below may be under attack:
22, 29, 37, 63, 66, 74,

Fig. 5.EyeSim GUI

The tool projects an eye which uses multiple ellipses and it is in 2D planar view. Each ellipses has its peculiar color, width, height. The height represents the latency of the node. The latency of the node reveals that for what time the legitimate node remains unconnected. To identify the state of each node three colors are used blue,red and green. A time window is used as the threshold. If the latency of the node is less than the threshold then the node is said to be not affected. If the node has the latency which is greater than the threshold then WAD engine is triggered. WAD engine determines the state of the node. Even if with higher latency no alarm is triggered then the nodes are classified as unconnected and are colored green. The nodes that are in the routing path of malicious nodes are termed as victim nodes and are highlighted with red color. The nodes that do not include in the routing path of malicious node are considered as unconnected and are colored green. The messages and alerts are produced in order to inform the user about the current network status so as to take some actions by the visualisation engine.
The administrator can see the list of nodes that belong to each category i.e. legitimate, unconnected, victim nodes.

VII. Conclusion

In this paper the proposed tool EyeSim is studied.The rate of cyber crime is increasing as the threats have been increased such as wormhole attack. These attacks are detected in sensor networks using this tool. It is basiclly a security visualisation tool. In this paper a trusted detectipon system which is visually assisted and is capable of monitoring and finding the security threat i.e. wormhole *attack is presented.*

References

[1] "ADLU: a novel anomaly detection algorithm for UWB WSNs" EURASIP journal on Information Security, no. 1, pp. 1-12-2014.

[2] G. Koien, "Security and privacy in the Internet Of Things: status and open issues" in Privacy and Security in Mobile Systems, May 2014.

[3] A .Lu, W. Wang, "Sybil Attack Detection through global topology pattern visualization" Information Visualization, vol. 10, Jan 2011.

[4] Q. Liao, Y. He, R. LI, "SAVE: Sensor Anomaly Visualization Engine," in IEEE Conference on VAST, Oct, 2011.

[5] "Visualization assisted detection of Sybil attacks in Wireless Networks", 3rd International Workshop.

[6] B. Parbat, A. K. Dwivedi, "Data Visualization Tools for WSNs: A glimpse. " International Journal of Computer Application, May 2010.

[7] "Applied Security Visualization", Pearson Education, 2009.

[8] "Data Visualisation: Graphical Techniques for Network Analysis", No Starch Press, Oct 2007.

[9] "Wireless Cyber Assets Discovery Visualization," in 5th International Conference, Heidelberg: Springer 2008.

[10] G. Abuaitah , "A security visualization tool for qualnet generated traffic traces", in 6th International Workshop, 2009. pp 111-118

[11]A. Lu, "Interactive Wormhole Detection in large scale WSNss", IEEE Symposium, 2006, pp. 99-106..

[12] W. Wang and B. Bhargava, “Visualization of wormholes in sensor networks,” in *ACM workshop on Wireless Security*. ACM Press, 2004, pp. 51–60.

[13] D. Keim, "Information visualization and data mining", IEEE transactions on visualization and computer graphics, Jan 2002, vol. 8.

[14] J. Mackinlay, "Readings in Information Visualization: Using vision to think", 1999.

[15] X. Chen, " Sensor network security: A survey", IEEE, vol. 11, 2009.

[16] Y. Sankarsubramanian, "Wireless sensor networks: A survey", vol. 38, March 2002