International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

A Simple Authentication Protocol for Secure Data Collection in Wireless Sensor Network

[1] Triveni Mane, [2] Raveendra.G
Dept. of Electronics and Communication
REVA Institute of Technology and Management, VTU, Bangalore, India
mtrivenibec@gmail.com, manjula@revainstitution.org

***Abstract*— For numerous applications large scale sensor network are used and data have been collected are used in process of making decision. Information that are from different origins over intervening nodes that collects information packets. A intervening malicious nodes may introduced by the attacker in the network and or disturbs present nodes. Therefore for making correct decision it is very difficult to providing high data trustworthiness. To find the trustworthiness of sensor data a key factor is represented by data provenance. In sensor network provenance management introduces various challenges like limited bandwidth and energy consumption, efficiency storage and secure transference. This paper prefers a light weight mechanism for securely sending of provenance for sensor input information. To encode provenance the suggested scheme depends on in-packet bloom filter. Here we used this efficient mechanism for verification of provenance and reconstruction of data at base station.**

***Keywords*—Provenance, encoding-decoding, Authentication key, malicious node**

I. INTRODUCTION

In numerous applications sensor networks are used for environmental monitoring, cyber physical infrastructure system, power grid etc. The source from immense number of sensor node produces data along with processed in network near to transitional leaps to the base station for outcome building process. The difference of input sources generates the needs to satisfy the input trustworthiness in that only authentic data is used in outcome building process. The origin of data indicates the important feature. This basic part is deciding the steadiness of sensor data. To assure data trustworthiness data sources are needed so that it is helpful in decision making process using trustworthy information. Input origin is a direct process to determine input steadiness, after all it compiles the history of the ownership and the operations implemented on the input. Base station track the forwarding path and source of an each information data. Origin for each packet must be taped however the main threats arises as result of bandwidth and compact storage energy restraints of sensor nodes. Therefore a lightweight provenance explication with limited overhead is necessary. Moreover, sensors usually act on, an environment which is normally untrusted, where may easily be influenced by attackers. Hence confidentiality, integrity and freshness of provenance are required to address the security. Our aim is to model an encoding and decoding mechanism for provenance that convince such security and performance desires.

II. NETWORK MODEL

A multi-hop wireless sensor network, consisting a base station which gathers information from the number of sensor nodes in the sensor network. The graph for this network is represented as a G(N,P), where the set of nodes and the set of links is N={ni|, 1<=i<=|N|} , and L respectively, and link L consisting an element $l_{i,j}$, ni and nj are the pair of nods that directly shares information with each other. Sensor nodes are static after placing it in network, but it may have dynamic routing paths overtime, e.g., because of node decline. After positioning nodes, each node in network provides detailed information to its neighboring(i.e., single hop) node and inform it to the BS. The BS then provides unique identifier to individual node as a node ID and a key Ki (symmetric cryptographic). In addition, a hash functions H ={h1, h2, . . . , hk} are transmit to the nodes for provenance implanting.

III PROPOSED SYSTEM

The complication of secure and tranference of efficient provenance and procedure for sensor networks is discussed. The strategy for provenance encoding is proposed whereby the provenance information from individual node on the route of a info packet securely inserted inside a bloom filter and that is sent together the information. After reception of the data packet from the BS it will then perform the decoding step by extracting data and then verification of the provenance information. In proposed system using key exchanging, cryptography, and

signature technique are used. So easily detect the suspicious data. In verify module detect the suspicious data and provenance data.

IV SCOPE OF THE WORK

In a multi-hop sensor network, info origin let the base station to track the origin and route that used for transmission of an each input packet. origin for individual packet must be listed, but important challenges that emerge because of dense storage, less energy and bandwidth of sensor nodes. Therefore, it is significant to formulate a light-weight provenance method with less overhead. Furthermore, sensors that are conduct frequently in an untrusted environment, where attacks may be possible. Thus, it is significant to direct security needs such as confidentiality, integrity of provenance.

V. ALGORITHM

Input: packets that are received with sequence seq and iBF ibf.Let N be the node set in the network, Let H be the hash functions set.

1. Initialization

Possible set nodes S← ∅

BFc ← 0 //For representing S.

2. To find the available nodes in the route and construct the representative BF

for individual node ni ∈ N **do**

vid$i$=generate VID(ni,seq)

if (vid$i$ is in ibf) **then**

S←S∪ni

insert vid$i$ intoBFc using hash function in H

end if

end for

3. verify BFc with the iBF at receiver side

if(BFc=ibf)**then**

return S //Origin has been determined//

else

return Null //Attack occurred //

end if

VI. SIMULATION RESULT

Here we used the network simulator(NS2) to implement and to test the proposed techniques. These are the graphs resulted after transmission of set of packets from source to the destination. Fig 1. shows the loss that is occurred while transmission of packet, this is the loss that occurred during reception of data by base station. According to the graph Initially there is no loss it maintains no loss but after some time few of the packet will get loss as shown in the graph then it maintains no loss. And the Fig 2. Which provides the resulting packet ratio that are delivered from sender source to the destination.

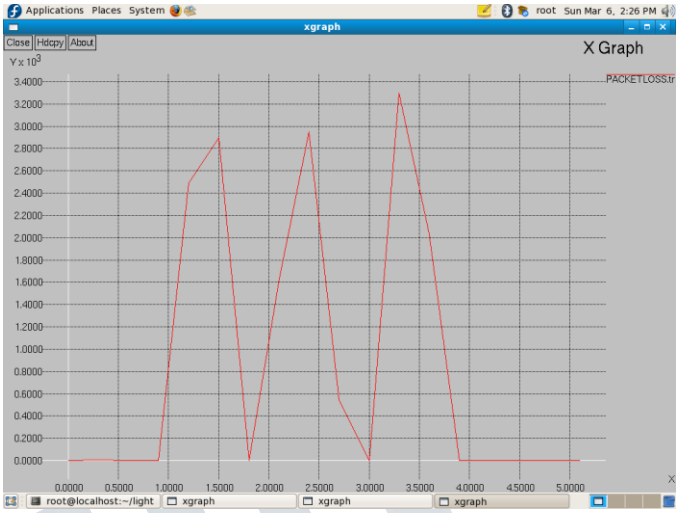

Fig 1:Packet loss(y-axis) Vs time(x-axis).

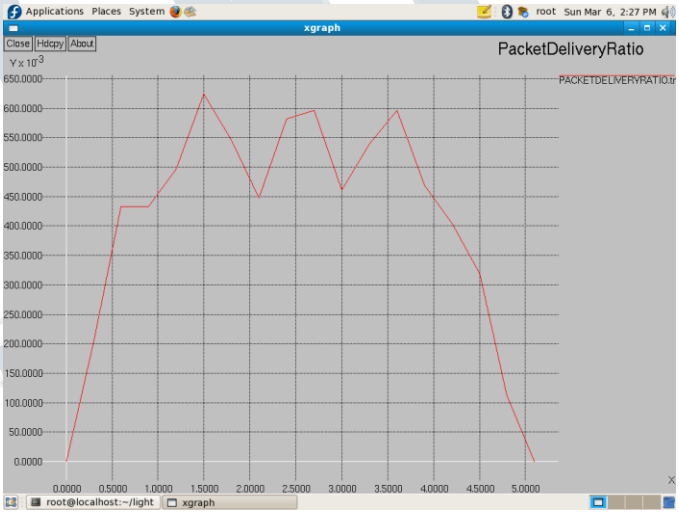

Fig 2: shows graph for packet delivery ratio.

VII. CONCLUSION

To avoid the problem caused by malicious node which is deployed, access by the hackers, we proposed new mechanism that explains the how to securely transmit provenance for sensor network, that new mechanism is namely light weight mechanism. Here in this we not only encodes the data but also we choose secure path in order to provide security for secure transmission of confidential information to BS. Therefore we encode selected path to avoid hacking. This scheme ensures the confidentiality, Freshness of provenance and integrity.

.

REFERENCES

[1]Salmin sultan, Elisa Bertino, Mohamed Shehab "A Lightweight Secure Scheme For Detecting Provenance Forgery And Packet Drop Attack In Wireless Sensor Networks" vol.12, No.3, may/june 2105.

[2]H.Lim,Y.Moon, Elisa Bertino, "Provenance Based Trustworthiness Assessment In Sensor Networks", seventh international workshop data management for sensor network,pp.2-7,2010.

[3]K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance Aware Storage System" Proc. USENIX Ann. Technical conf,pp.4-4,2006.

[4]Y. Simmhan, B. Plale, D. Gannon, "A survey of data provenance in E-Science," ACM SIGMOD Record, vol. 34,pp.31-36, 2005.

[5]S. Sultana, and M. Shehab, "A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011.

[6] A. Kirsch and M. Mitzenmacher, "Distance-Sensitive Bloom Filters," Proc. Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

[7] C. Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wiesmaier , "In-Packet Bloom Filters: Design and Networking Applications," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.

[8] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052, June 2012.