International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 16th July 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-5

Title: Efficient Forgery Attack, Packet Drop and Detection Methods in Wireless Sensor Network.

Volume 06, Issue 05, Page No: 1866 – 1876.

Paper Authors

***K.PAVANI, ANITHAMMA, BEEMAL.**

* Dept of CSE, Shri Shiridi Sai Institute of Science and Engineering.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

EFFICIENT FORGERY ATTACK, PACKET DROP AND DETECTION METHODS IN WIRELESS SENSOR NETWORK

[1]K.PAVANI, [2] ANITHAMMA, [3]BEEMAL

[1]PG Scholar, Dept of CSE, Shri Shiridi Sai Institute of Science and Engineering, AP, India
[2]Assistant Professor, Dept of CSE, Shri Shiridi Sai Institute of Science and Engineering, AP, India
[3]Assistant Professor, Dept of CSE, Shri Shiridi Sai Institute of Science and Engineering, Ap, India

ABSTRACT

Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision-making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. In this paper, we propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the, lightweight secure provenance scheme in detecting packet forgery and loss attacks.

INTRODUCTION

As of late, the harmful progress of versatile registering objects comprises portable PCs, individual digital assistants (PDAs) and handheld evolved objects, has motivate a innovative alterations in the processing scene. Processing environment every man or woman patron uses the equal time, by means of making use of different digital phases by way of which they can get to all of the required expertise. It's unrealistic for the universal items to get wired process to interface with different pervasive objects. It is predominant to include far off process because the interconnection procedure.

1.1 Importance of Mobile Ad-Hoc NetworksMobile Ad-hoc Networks

(MANETS), an accumulation of far flung moveable hubs are prepared for speak me with one a different without a utilization of concentrated organization. Despite the truth that MANETS present unhindered versatility and availability to the purchasers, they likewise go about as switches for sending bundles considering the fact that of their restricted transmission stages. MANETS are likewise termed as Infrastructure less systems administration because the versatile hubs in the system gradually installed guidance among themselves in their possess distinct approach on the fly. As each one of the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

vital indicators expertise an information switch ability compelled faraway connections, it's more inclined to physical protection dangers. These versatile hubs can wander freely and can move in any course. Hubs can correspond with the various hubs within their reaches, although the hubs that aren't within the correspondence extent use neighboring hubs to speak with one yet another. The portable in particular appointed procedure (MANETs) has the accompanying elements:

- Untrustworthy of wireless links between nodes.
- Due to the continuous motion of nodes. The topology of the MANETS changes constantly
- It is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Hence, any protection solution with a static configuration would not be adequate for a dynamically changing topology. Because of the boundaries of the lots of the routing protocols devised for MANETS, leaves the attackers to have a colossal have an impact on the network with just one or two compromising nodes. Hence, the IDS which might be developed should provide more advantageous security degree for the community. If MANETS can realize the intruders as soon as they can enter the network we can get rid of the capabilities damages that can be caused via the compromised nodes on the preliminary stages itself.

MANETS is emerging study areas with sensible functions. MANETS are vulnerable to attacks on account that of their dynamic topology, open medium, restricted capability. Also routing plays an primary position in the protection for the entire community. In MANETs, each node plays an important role not simplest as a host but in addition as a router. Each and every node participates in an ad-hoc routing protocol which permits discovering multi-hop paths inside the network. Despite the fact that, this model presents bendy ways for verbal exchange, protection is a central obstacle. The possible assaults can variety from passive eavesdropping to energetic interference. Any attacker can take heed to or alter the visitors and could attempt to masquerade as some of the members. Cryptography and certificate established authentication maybe complex in MANETS seeing that of the absence of vital help infrastructure.

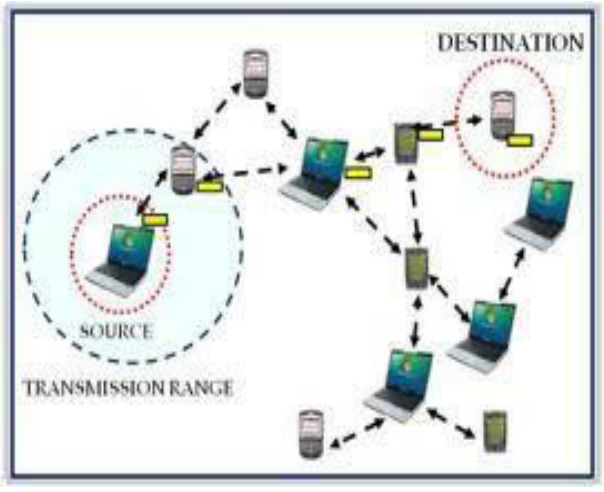


Fig 1.1: Structure of MANET

How MANET Works?

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors. Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features.

Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol(RMP)
- ProactiveMANETProtocol(PMP)

If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed.

The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best effort multicast forwarding function. The use of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues.

The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing research topics related to MANET environments.

LITERATURE SURVEY

In this paper, they discuss security issues and their present courses of action in the compact extemporaneous framework. There are different security threats that irritate the change of the MANETs because of its feeble nature. They prompt and separate the standard issues (vulnerabilities) in the flexible extemporaneous frameworks, which have made it much simple to encounter the evil impacts of strikes than the traditional wired framework. By then they discuss the security criteria of the flexible off the cuff framework and present the essential and basic ambush sorts that exist in MANETs. Finally they give the response for study the present security for the compact extraordinarily named framework.

2.1 A Secure On-Demand Routing Protocol for Ad Hoc Networks

A specially appointed system is a gathering of remote versatile PCs (or hubs), in which singular hubs collaborate by sending parcels for one another to permit hubs to impart past direct remote transmission range. Specially appointed systems administration has by and large considered the directing issues in a restricted setting, expecting a trusted domain. In this paper, they present assaults against the directing in Mobile specially appointed systems, and they introduce the outline and execution assessment of another secure on-interest steering convention in impromptu systems called Ariadne. It keeps vindictive or bargained hubs from messing with the uncompromised courses comprising of

uncompromised hubs, furthermore counteracts numerous sorts of DOS assaults. Also, Ariadne is effective, utilizing just exceedingly productive symmetric cryptography primitives.

2.2 Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks

The definition for Mobile Ad hoc Network of Networks (MANETs) are a social occasion of colossal free remote centers granting on an appropriated premise in a heterogeneous space with no predefined system. Each center point extemporaneous framework having its own organization System. Suggestion ITU-T M.3400 security organization containing foresight, security association and acknowledgment of noxious center points. Recovery is thought to be one of the main problems in MANETs. In this paper they propose a "Behavior acknowledgment figuring" joined with farthest point cryptography mechanized validations to satisfy balancing activity and recognizable proof to securely manage our structure.

2.3 Dynamic Source Routing in Ad hoc Wireless Networks, in Mobile Computing

An ad hoc network system is an accumulation of remote versatile hosts framing a transitory system without the guide of any incorporated organization and set up framework. In such a conditions, it might be essential for every portable hub host to enroll the counsel of alternate hosts in sending parcel from source to destination. Because of its constrained scope of every versatile hub host's remote transmissions. This paper exhibits a DSR Protocol (element source directing convention) for Ad-hoc systems. This convention adjusts directing changes immediately when versatile hub moves starting with one place then onto the next yet it requires a practically no overhead amid periods in which portable hubs moves gradually.
In view of the outcomes from a bundle level reenactment of portable hubs working in a specially appointed system, the DSR convention performs exceptionally well in an alternate ecological conditions, for example, development rates and host thickness. For everything except the most elevated rates of developments in hosts is mimicked, the overhead of the convention is entirely low, tumbling to only 1% of aggregate information bundles transmitted for moderate development rates in a system of 24 portable hosts.

2.4 Detecting Misbehaving Nodes in MANETS

Specially appointed systems are decentralized and unstructured frameworks organization show that depends on upon the center points support is key framework functionalities, for instance, coordinating and medium access. In this paper, they developed a model in perspective of the Sequential Probability Ratio Test to depict how centers can separate between the courses that consolidate poisonous center points (defiled courses) and courses that don't. The rule playing purpose of the model is that the amount of recognitions expected to survey a course require not be bound and determined early, which suits well the component behavior of the uniquely delegated frameworks. They format a united and a kept approach to recognize malignant centers on

courses perceived by the model. They exhibits that the constrained approach is not only the better basic choice for exceptionally selected frameworks moreover it gives achieves a more exact presentation of misbehaving centers while getting low false positives and low false negatives.

3.1 Existing System

Various protocols are available for the data aggregation while forwarding the packets. They are mainly classified as tree-based approach, cluster-based approach and structure-less approach.

Shortest Path Tree (SPT) Algorithm

It is a tree-based routing approach. It usually depends on hierarchical organization of the nodes. It uses a very simple strategy to construct the tree structure. Each source sends its information to the sink along the shortest path . Where these paths overlap for different sources, they are combined to form the aggregation tree. It has static.

Greedy Incremental Tree (GIT) Algorithm

It is also a tree-based approach. It is based on Direct Diffusion Approach. It establishes an energyefficient path and greedily attaches other sources onto the established path. The information is routed using the shortest path in the tree. Whenever a new branch is created new aggregation point is also selected.

Tiny AGgregation (TAG) Service

In the TAG algorithm, parents notify their children about the waiting time for gathering all the data before transmitting it so the sleeping schedule of the nodes can be adjusted accordingly. It makes use of shortest path to route the It requires large number of message exchange to construct and maintain a tree.

Information Fusion-based Role Assignment (InFRA) Algorithm

It is a cluster-based approach. The algorithm aims at building the shortest path tree that maximizes information fusion. Thus, once clusters are formed, cluster-heads choose the shortest path to the sink node that also maximizes information fusion by using the aggregated coordinators distance. For each new event that arises in the network, the information about the event must be flooded throughout the network to inform other nodes about its occurrence and to update the aggregated coordinators-distance. This increases the communication cost of the algorithm and, thus, limits its scalability.

Data-Aware AnyCast (DAA) Algorithm

It is a structure-less approach. Uses anycast to forward packets to one-hop neighbors that have packets for aggregation. It has mechanisms for increasing the chance of packets meeting at the same node (spatial aggregation) and at the same time (temporal aggregation).It does not guarantee aggregation of all packets, the cost of transmitting packets with no aggregation increases in larger networks.

- Recent research highlighted the key contribution of provenance in systems

where the use of untrustworthy data may lead to catastrophic failures (e.g., SCADA systems). Although provenance modeling, collection, and querying have been studied extensively for workflows and curated databases, provenance in sensor networks has not been properly addressed.

- Pedigree captures provenance for network packets in the form of per packet tags that store a history of all nodes and processes that manipulated the packet.

- Hasan et al. propose a chain model of provenance and ensure integrity and confidentiality through encryption, checksum and incremental chained signature mechanism.

  Chong et al. embed the provenance of data source within the data set.

  Disadvantages of Existing System:

  - Major disadvantage of this scheme is the use of untrustworthy data at the nodes may create the catastrophic failures, means sudden and total failure from which recovery is impoassible.
  - Sensor networks are not been properly addressed.
  - It does not guarantee aggregation of all packets, the cost of transmitting packets with no aggregation increases in larger networks.
  - Employs separate transmission channels for data and provenance.

3.2 Proposed System

We investigate the problem of secure and efficient provenance transmission and processing for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes.Our goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node.

Collaborator: A node that detects an event and reports the gathered data to a coordinator node. Coordinator: A node that also detects an event and is responsible for gathering all the gathered data sent by collaborator nodes, aggregating them and sending the result toward the sink node. Sink: A node interested in receiving data from a set of coordinator and collaborator nodes. Relay: A node that forwards data toward the sink. The working of model is divided into following phases:

1. First step is to calculate the distance from the sink node to other nodes of the network.
2. At the first event, cluster head is selected which is closer to sink node and it is called as coordinator and the remaining node that detect the same event are named as collaborator.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3. The routes are created by choosing the best neighbor which is at minimum distance from sink node and accordingly distance from sink node is updated.
4. Route repair mechanism: Here if the sender node receives ACK from the node within the pre-determined timeout, it will assume that the node is alive else new node is selected. At appoint when one of the two node is to be selected node with highest energy is selected.

3.2.1 Advantages of Poposed System

- We use only fast message authentication code (MAC) schemes and Bloom filters, which are fixed-size data structures that compactly represent provenance. Bloom filters make efficient usage of bandwidth, and they yield low error rates in practice.
- We formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.
- We propose an in-packet Bloom filter (iBF) provenance-encoding scheme.
- We design efficient techniques for provenance decoding and verification at the base station.
- We extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.
- We perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.

Architecture Diagram

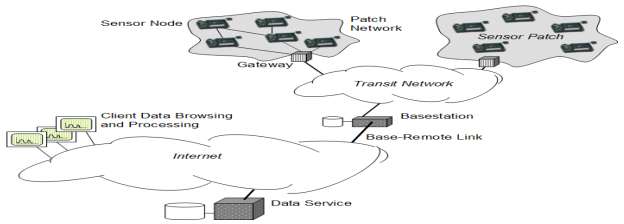


Fig 3.1 System Architecture

In this architecture data service is an provision and distribution model in which data files are made available to customers over a network, typically in the network. Data services are similar to software as a service in that the information is stored in the cloud and is accessible by a wide range. Through internet client data browsing and processing is done. and base station is receive the information through base-remote link and trasmit through the transit network. Through gateway sensor node data is transferring to sensor nodes and sensor patch to destination.

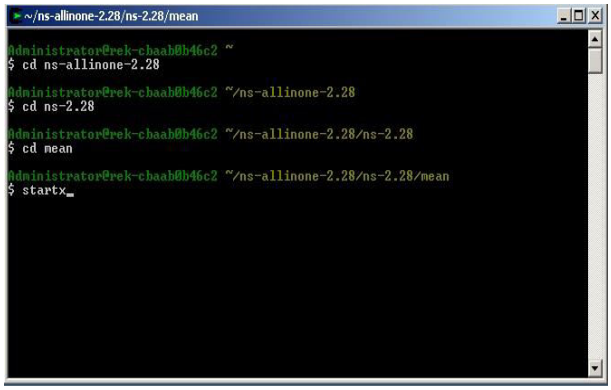
In this chapter the practical interface is discussed. Execution steps are explained. I can explain the execution steps with sample screens.

7.1 Results

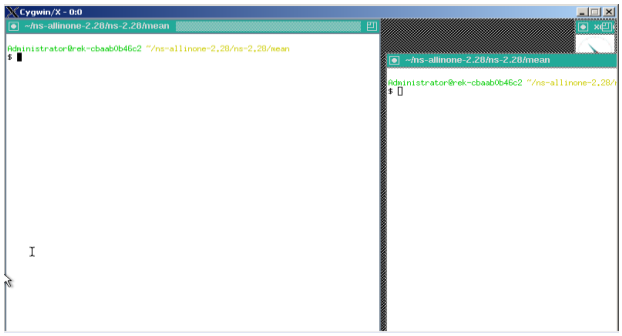
The result section shows the execution results of the project. Every node is send data to the perticular channel and all channels are send data to the destination in this we can calculate the distance of every node.

7.2 Sample Screens

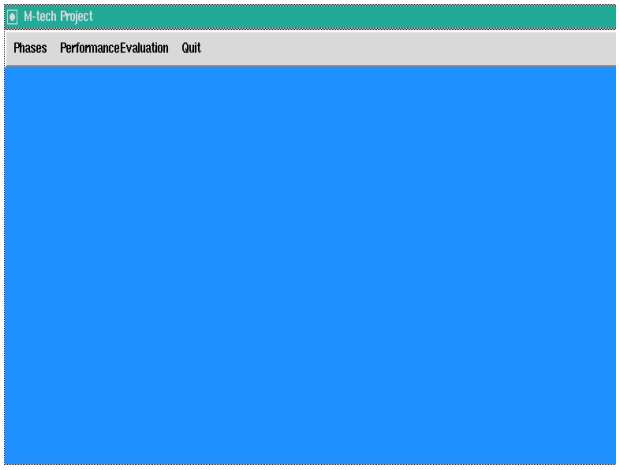
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org



This screen shot explains the process of coding. Change the path to ns-allinone 2.28/ns-2.28. Run the command.

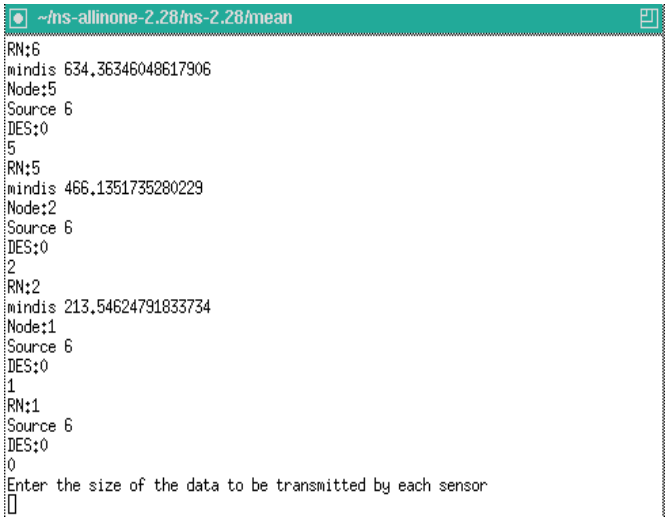


This screen shot explains run the command ./ wish.exe main.tcl. This ccommand is used in the execution steps, and to run the project.



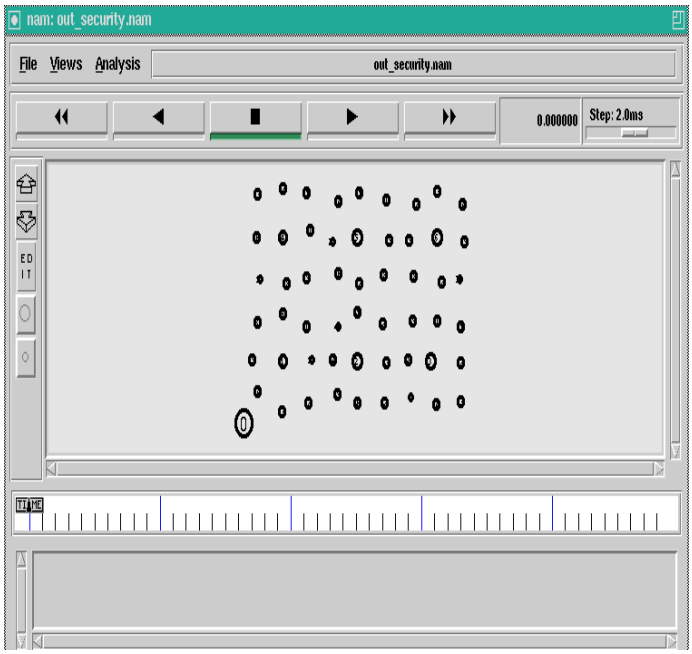
And then open the new window m.tech project contaions phase light wieght.

This screen shot explains the phases of the projet that phase is lightweight.



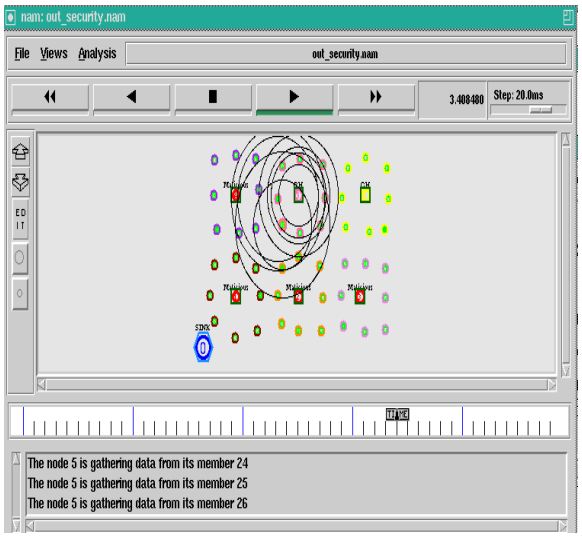
This screen shot explains the enter the size of the data to be trasmitted by each sensor.

That data is received the source node verify and then transmit the destination node.

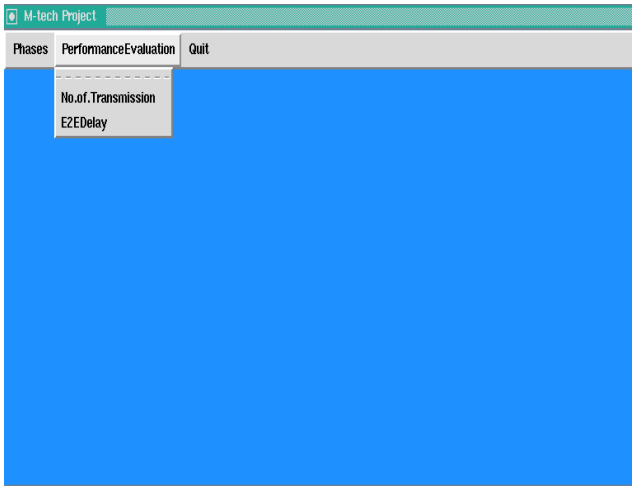


In this i can expalin the execution strating stage. To calculate the time also.

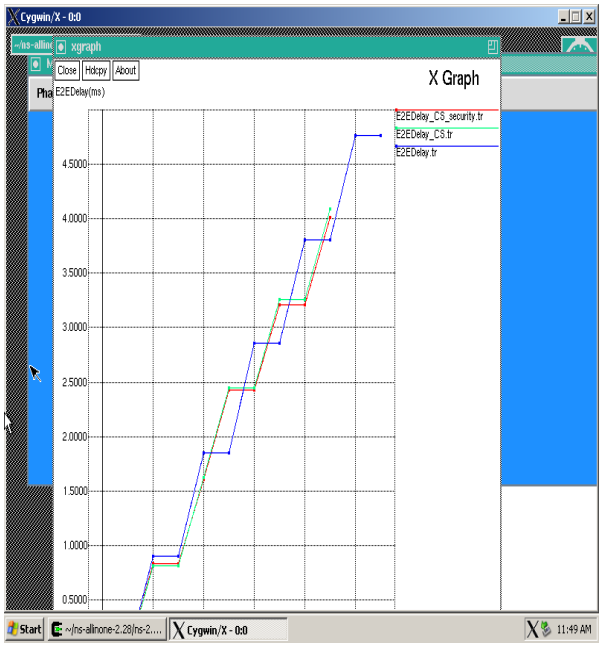
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org



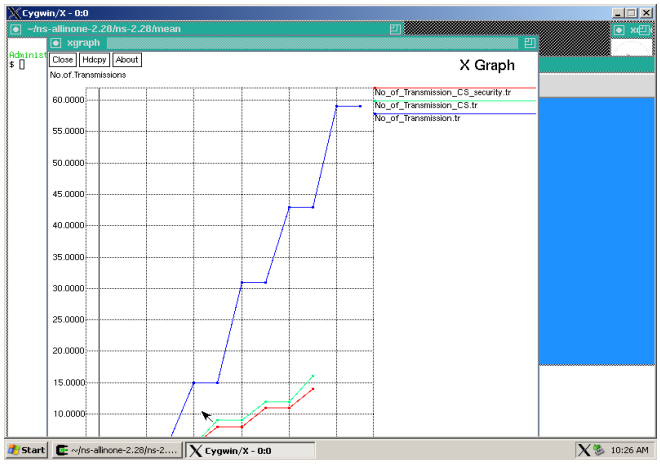
In this every node is gathering from its members sink node is transmitted data, sink node means basestation. Cluster head is transmitting the collected information to the sink node. Every node is send data to the perticular channel and all channels are send data to the destination in this we can calculate the distance of every node. Base sation to data is transferred to clusters and those clusters having cluster head and then all cluster head are traferring data to destination. At that time malicious node is compremising the other nodes. We identify the malicious nodes.



This screen shot explains the performace evaluation. In performance evaluation I can verify the number of transmissions and E2E delay.



In this End-to-end packet drop rate for various percentages of malicious nodes deployed in the network.



In this we can explain the number of transmissions.

Summary

I can detect the malicious nodes in the network and then securely transmitting data to the base station to destination. I can identify the malicious nodes in the network and then data is seucrely transmitted to the destination.

CHAPTER – 8

CONCLUSION & FUTURE WORK

I addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate dataprovenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, I plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

[1] Villas L.A, Boukerche A, Ramos H.S, De and Loureiro A.A.F (2013)"DRINA:A Lightweight Aggregation in Wireless Sensor Networks," IEEETrans.,on computers, vol.62 No.4, pp 676-689.,2013.

[2] Al-Karaki J, Ul-Mustafa R, and Kamal A , "Data Aggregation in Wireless Sensor Networks —Exact and Approximate Algorithms,"Proc. High Performance Switching and Routing Workshop (HPSR '04),pp. 241-245,2004.

[3] Akyildiz I.F, Su W, Sankarasubramaniam Y, and Cyirci E, "Wireless Sensor Networks: A Survey," Computer Networks, vol.38, no. 4, pp. 393-422,2002.

[4] Anastasi G, Conti M, Francesco M, and Passarella A , "Energy Conservation in Wireless Sensor Networks: A Survey," Ad Hoc Networks, vol.7,no. 3, pp. 537- 568,2009. http://dx.doi.org/10.1016/j.adhoc.2008.06.003.

[5] Chandrakasan A.P, Smith A.C, and Heinzelman W.B , "An Application-Specific Protocol Architecture for Wireless Microsensor Networks,"IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670,2002.

[6] Krishnamachari B, Estrin D, and Wicker S.B, "The Impact of Data Aggregation in Wireless Sensor Networks," Proc. 22nd Int'l Conf. Distributed Computing Systems (ICDCSW '02), pp. 575-578,2005.

[7] Nakamura E.F, Loureiro A.A.F, and Frery A.C "Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications," ACM Computing Surveys, vol. 39, no. 3, pp. 9-1/9-55,2007.

[8] Romer K and Mattern F, "The Design Space of Wireless Sensor Networks,"IEEE Wireless Comm., vol. 11, no. 6, pp. 54-61,2004.

[9] Villas L.A, Boukerche A, Araujo R.B, and Loureiro A.A (2009), "A Reliable and ACM Int'l Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), pp. 245-252.

[10] Younis O, Krunz M, and Ramasubramanina S, "Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges," IEEE Network, vol. 20, no. 3, pp. 20- 25,2006.

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10,2010, pp. 216–222.

[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowl- edgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile *ad-hoc* commu- nications in AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323,2004.

[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbe-haviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbe- haviour in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.