Identifying Packet Loss In Wireless Sensor Network

Subramani. S
Computer science Engineering,
Sethu Institute of Technology, Pullor
Kariappati, Virudhunagar.

Jeyalakshmi. C
Assistant Professor
Computer science Engineering
Sethu Institute of Technology, Pullor
Kariappati, Virudhunagar

Abstract— Packet loss is the failure of one or more transmitted packets to arrive at their destination. Packet loss minimizes the Packet Delivery Ratio. Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading. Packet loss is possible in wireless sensor network. So that the intruders can be easily capture the data .Identifying the dropping packet and misbehaving activities are the most necessary measures for secure transmission in it. Without a certificate a node cannot participate in the transmission. This paper uses Location based algorithm is to identify the intruders which is a packet dropper or modifier. If a new node is entered into the WSN, It cannot participate in the transmission process until it does not get the certificate. After receiving the certificate from the sink node it can also participate in the transmission. In this SHA1Algorithm and Rivest, Shamir and Adleman (RSA) are used to generate the certificate for each node in WSN using private and public key.

Keywords— WSN, Packet loss, SHA1, RSA, Location based.

1 INTRODUCTION

A Wireless Sensor Network (WSN) [6] is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations." The nodes in the network are connected via Wireless communication channels. The power for each sensor node is derived from the electric utility or from a battery.

A Sensor Network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena.

A packet [7] is one unit of binary data capable of being routed through a computer network. Packet dropping [4] is a compromised node which drops all or some of the packets that is supposed to forward.

2 RELATEDWORK

Sakshi Kausha et al(2010) [1]- propose a an algorithm for optimization of adaptive buffer allocation scheme for traffic based on loss of consecutive packets in data-stream and buffer occupancy level. Buffer is designed to allow the input traffic to be partitioned into different priority classes and based on the input traffic behavior it controls the threshold dynamically. In this Adaptive Partial Buffer Sharing (ADPBS) packet loss control scheme for two and multiple priority classes in congested networks. ADPBS manages to reduce consecutive packet loss as compared to SPBS and FIFO queues due to its adaptive threshold nature.

Cirstea.C et al(2012) [3]- analyze the importance of packet loss consideration (PLC) within inter node communication of a WSN. They evaluate the link quality between network nodes based on the link packet loss and not on the received signal strength indicator (RSSI).They propose a network initialization phase where all nodes gather information about the link packet loss from all neighbors. Using this information each node will choose the attending cluster head (CH) based on the smallest packet loss rather than on the highest RSSI. Matlab simulations show that considering packet loss in choosing the best communication path has a significant impact on reducing the energy consumption of the network as well as increasing network throughput.

Orellana-Romero.E et al(2011)[14]- propose a Sim-LIT, a framework for the simulation of packet loss effects on the quality of non-coded or coded still images transported over wireless sensor networks. The tool is focused on image quality assessment and it can be used to evaluate error resilience during image communications. In this first version the evaluation of block interleaving methods is provided. Sim-LIT is highly configurable, providing several options and additional tools. It may be useful to rapidly evaluate interleaving algorithms, or other techniques, or to perform extensive tests considering various image files and loss patterns. Through different simulations we demonstrate the potential of Sim-LIT as a tool for supporting research activities on the image processing and wireless sensor networks domains.

Faisal Ghias Mir et al (2012)-[2] propose Re-ECN is a resource sharing framework that enables such resource usage accountability, employing enforcement points in the network. These are often described as packet droppers at or near the egress of an end-to-end path. This paper presents a packet dropper design that allows implementing the required congestion declaration enforcement efficiently. The dropping algorithm only switches to Observation Mode once the aggregate trend crosses some pre-configured threshold suggesting cheating flows. The dropper builds the necessary state for identifying misbehaving flows. The limitation is time based sampling with lower processing footprint in the data path but with lower accuracy.

3 PROPOSED SYSTEM

The network is formed with thirty nodes and packet is generated for all nodes. The sender and receiver are selected within the thirty nodes. The sender sends the packet to the receiver by using the shortest path algorithm. Then the performance is analyzed for the packet dropping and modification. It request to the sink node to participate in the transmission. Then certificate is generated to the new node. Then the new node can participate in the transmission.

The certificate is given to all the nodes by SHA1 and RSA Algorithm. In this one node acts as a sender and another node acts as a receiver.

Node(0)
192.26.2.1
c4dfd145e649849eb4a66f83c052a8de
00:11:11:19:B1:EA
1
1

Figure 2: Certificate Generation for node 0

The sender selects the file to transmit. The files are divided into no of packets. The data packets are transferred through the shortest path from the sender to the receiver. The packet identification is done and forwarded through the shortest path.

3.2 SHA1Algorithm

SHA1 stands for “Secure Hashing Algorithm” . It is a hashing algorithm SHA0 and was first published in 1995. SHA1 is currently the most widely used SHA hash function; SHA1 outputs a 160-bit digest of any sized file or input. In construction. It uses a 512 bit block size and has a maximum message size of 2 - 1 bits.

Step1: Padding

Pad the message with a single one followed by zeroes until the final block has 448 bits.

Append the size of the original message as an unsigned 64 bit integer.

Step2: Initialize the 5 hash blocks

(h0,h1,h2,h3,h4) to the specific constants defined in the SHA1 standard.

Step3: Hash (for each 512-bit Block)

Allocate an 80 word array for the message schedule

Set the first 16 words to be the 512-bit block split into 16 words.

The rest of the words are generated using the following algorithm

Step4:

Output the concatenation (h0, h1, h2, h3, h4) which is the message digest.

3.3 RSA Algorithm

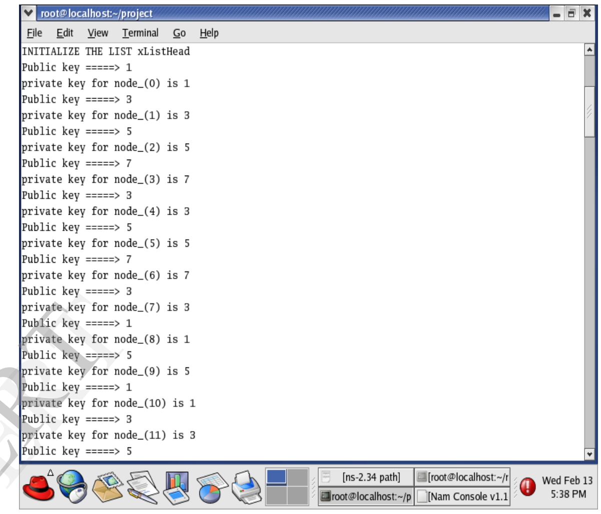
RSA stands for RonRivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1977[5]. The private key is used to decrypt text that has been encrypted with the public key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
2. Compute $n = pq$.
3. Compute $\varphi(n) = (p–1)(q–1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and greatest common divisor of $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime.
5. Determine d as:

   $d \equiv e^{-1} \pmod{\varphi(n)}$ i.e., d is the multiplicative inverse of e mod $\varphi(n)$.

4 EXPERIMENTAL RESULTS

In figure 3 shows the assignment of public key and private key for the thirty nodes.



```
INITIALIZE THE LIST xListHead
Public key =====> 1
private key for node_(0) is 1
Public key =====> 3
private key for node_(1) is 3
Public key =====> 5
private key for node_(2) is 5
Public key =====> 7
private key for node_(3) is 7
Public key =====> 3
private key for node_(4) is 3
Public key =====> 5
private key for node_(5) is 5
Public key =====> 7
private key for node_(6) is 7
Public key =====> 3
private key for node_(7) is 3
Public key =====> 1
private key for node_(8) is 1
Public key =====> 5
private key for node_(9) is 5
Public key =====> 1
private key for node_(10) is 1
Public key =====> 3
private key for node_(11) is 3
Public key =====> 5
```

Figure 3: Private Key Assignment

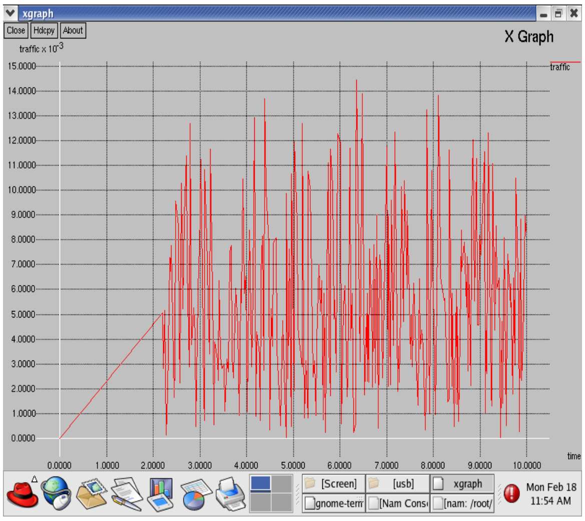


Figure 4: Traffic

In figure 4 shows the traffic analysis compared to the existing system Our Traffic analysis is less compared to the existing system

In figure5 shows packet delivery ratio is higher in our system than existing system. Thus the packet dropping and modification is minimized.

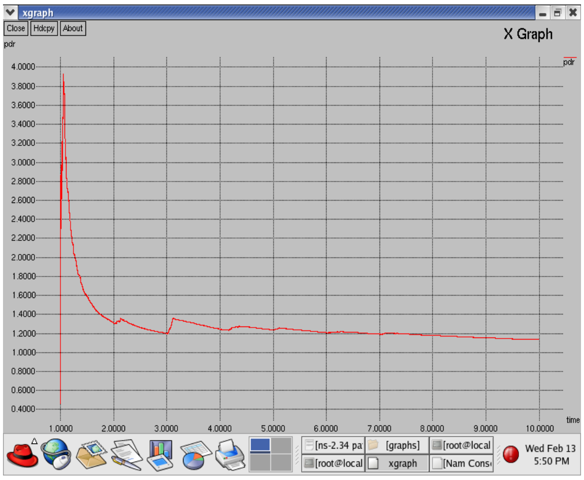


Figure 5: Packet delivery ratio

In Figure 6 shows the comparison of our system with existing system in Wireless Sensor Networks. Packet loss is reduced in our system than the existing system

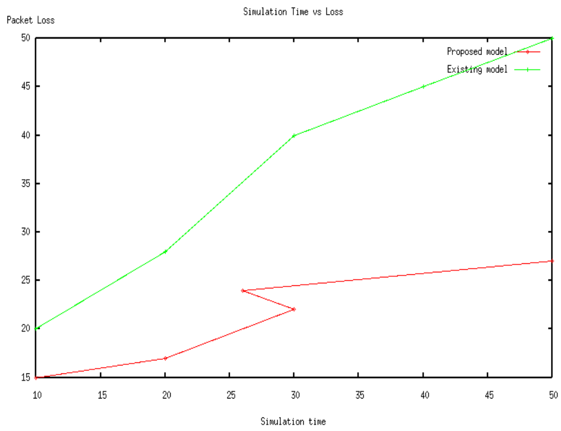


Figure 6: Comparison for packet loss

5 CONCLUSION

We design a typical deployment of sensor nodes with thirty numbers of nodes which are randomly deployed. The SHA1 and RSA algorithm is used to generate the certificate for the presented node. Certificate is generated to the each node. The packet identification is done and forwarded through the shortest path. The packet delivery ratio is increased. The packet dropper or modifiers are identified to be present in the network. If the packet dropper or modifiers are found in the network, the sink node gives the certificate again to the packet dropper or modifier node to participate in the transmission. In this the packet loss is reduced

REFERENCES

[1] Sakshi Kausha, R.K Sharma "Modeling and Analysis of Adaptive Buffer Sharing Scheme for Consecutive Packet Loss Reduction in Broadband Networks" May 2010

[2] Faisal Ghias Mir, Dirk Kutscher, Marcus Brunner and Rolf Winter "An EfficientDropper Design for Implementing Capacity Sharing with Congestion Exposure" IEEE Globecom 2011 proceedings.

[3] Cirstea,C Cernaianu,M. Gontean,A "Packet loss analysis in wireless sensor networks routing protocols" 2012

[4] http://en.wikipedia.org/wiki/Packet_loss

[5] http://en.wikipedia.org/wiki/RSA_(algorithm)

[6] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks" 2010

[7] W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in AdHoc Networks: A Multi-Dimensional Trust Management Approach," Proc. 11th Int'l Conf.

Mobile Data Management (MDM '10), 2010.

[8] T.H. Hai and E.N. Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-Hops Neighbor Knowledge," Proc. IEEE Seventh Int'l Symp Network Computing and Applications (NCA '08), 2008

[9] I.Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), 2008.

[10] X. Zhang, A. Jain, and A. Perrig, "Packet-Dropping Adversary Identification for Data Plane Security," Proc. ACM CONEXT Conf. (CoNEXT '08), 2008.

[11] K. Ioannis, T. Dimitriou, and F.C.Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," Proc. 13th European Wireless Conf., 2007.

[12] F. Ye, H. Yang, and Z. Liu, "Catching Moles in Sensor Networks,"Proc 27th Int'l Conf. Distributed Computing Systems (ICDCS '07), 2007.

[13] Orellana-Romero,E. SanMartin-Hernandez.J DuranFaundez,C. Lecuire.V Aguilera, C. "Sim-LIT: A Simulation Framework for Image Quality Assessment in Wireless Visual Sensor Networks under Packet Loss Conditions"