Increasing Packet Delivery Ratio in Wireless Sensor Network

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

Abstract— A Wireless Sensor Network (WSN) is a collection of nodes organized into a cooperative network. Each node consists of processing capability which acts as transceiver. Packet dropping is a compromised node which drops all or some of the packets that is supposed to forward. Packet modification is a compromised node which modifies all or some of the packets that is supposed to forward. Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi hop sensor networks. In this Message Digest5 Pure (MD5-Pure) and Rivest, Shamir and Adleman (RSA) algorithm are used to generate the certificate for each node in WSN using private and public key. Without a certificate a node cannot participate in the transmission. The 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. The packet delivery ratio is increased.

Keywords— WSN, Packet dropper, Packet modifier, MD5Pure, 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.

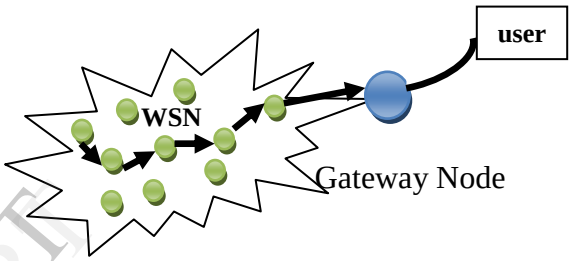

Figure 1.1: Wireless Sensor Network

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 is a compromised node which drops all or some of the packets that is supposed to forward. Packet modification is a compromised node which modifies all or some of the packets that is supposed to forward. It may also modify the data it generates to protect itself from being identified or to accuse other nodes.

2 RELATEDWORK

Mohamed Elsalih Mahmoud et al (2010)-[5] propose a credit-based mechanism that uses credits to stimulate the rational packet

droppers to cooperate, and uses reputation system to identify the irrational ones. Payment receipts are processed to reward the cooperative nodes, and to detect the broken links so that a reputation system can be built to identify the irrational packet droppers. In DRIPO, payment receipts are processed to extract financial information to update the nodes' credit accounts, and contextual information such as broken links to build up a reputation system to identify the irrational packet droppers. The authors identified the packet droppers.

Xiaoqi Li et al(2010)-[4] propose a idea of a trust model in subjective logic into the security solutions of MANETs. The trust and trust relationship among nodes can be represented, calculated and combined using an item opinion. If one node performs normal communications, its opinion from other nodes' points of view can be increased; otherwise, if one node performs some malicious behaviors, it will be ultimately denied by the whole network. A trust recommendation mechanism is also designed to exchange trust information among nodes. The salient feature of TAODV is that using trust relationships among nodes, there is no need for a node to request and verify certificates all the time In our TAODV routing protocol, nodes can cooperate together to obtain an objective opinion about another node' trustworthiness. They can also perform trusted routing behaviors according to the trust relationship among them. With an opinion threshold, nodes can flexibly choose whether and how to perform cryptographic operations. Therefore, the computational overheads are reduced without the need of requesting and verifying certificates at every routing operation. In summary, our trusted AODV routing protocol is a more light-weighted but more flexible security solution than other cryptography and authentication designs. The optimization is not done fast in it.

Francesco Saverio Proto et al (2011)-[3] proposes a fully distributed trust-based routing framework, tightly integrated with OLSR, which is the most exploited routing protocol in real world wireless community networks. The framework, designed to be modular for easy upgrade, relies on active probes, hidden in the normal data traffic through adaptation of Steganography techniques. The combination of path-wise measurements into distributed trust framework. The authors identified the misbehaving nodes.

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.

Mehdi Keshavarz et al (2012)-[1] propose Free-riding by packet dropping issues for the establishment and survivability of the open multi-hop wireless networks. In this paper, they focuses on the data packet dropping in the Mobile Ad-hoc Network. The author uses a technique to detect misbehavior in packet forwarding. The ambiguous collisions, receiver collisions, and limited transmission power are avoided in it. They identify the packet dropping nodes not the modifier nodes.

3 PROPOSED SYSTEM

The network is formed with twenty nodes and packet is generated for all nodes. Without a certificate no node can participate in the transmission. The sender and receiver are selected within the twenty 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. If a new node enters into the network, it cannot participate in the transmission because the new node doesn't have the certificate. 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 MD5 pure and RSA Algorithm. In this one node acts as a sender and another node acts as a receiver.

Node(3)
192.27.2.1
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.

The location based algorithm is used to identify the node which is entering without the certification. If the certification is not provided the node is identify as the dropper and modifier.

If a new node enters into the network, it cannot participate in the transmission because the new node doesn't have the certificate it request to the sink node to participate in the transmission. The certificate is generated to the new node. Then the new node is participated in the transmission

3.2 MD5Pure Algorithm

Step 1 – append padded bits:

- The message is padded so that its length is congruent to 448, modulo 512 bits long which is extended to 64 bit. A single "1" "0" bit is appended to the message.

Step 2 – append length:

- A 64 bit representation of b is appended and resulting message length is 512 bits.

Step 3 – Initialize MD Buffer

- A four-word buffer (A, B, C, D) is used to compute the message digest which is 32 bit register.

Step 4 – Process message in 16-word blocks.

- Four auxiliary functions take input as three 32-bit words, produce one 32-bit word output.

Step 5 – output

- The message digest produced as output is A, B, C, D. which begins with the low-order byte of A, and end with the high-order byte of D.

The difficulty of coming up with two messages with the same message digest is on the order of 2^64 operations.

3.3 RSA Algorithm

RSA stands for RonRivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1977. 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 MAC address for the twenty nodes. In figure 4 shows deployment of twenty nodes containing the sender node and receiver node and the certificate is generated for Node3.

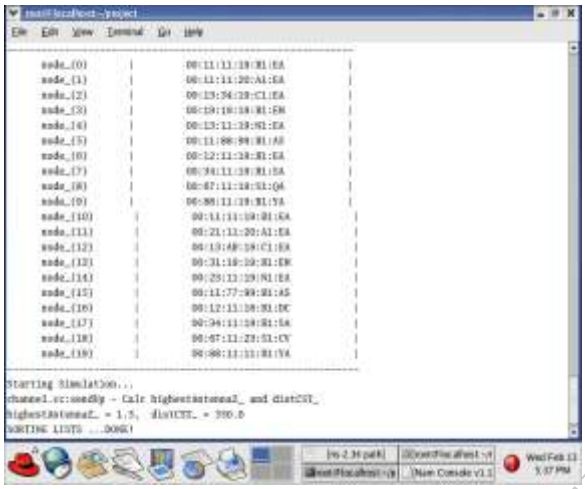

Figure 3: MAC Address Assignment

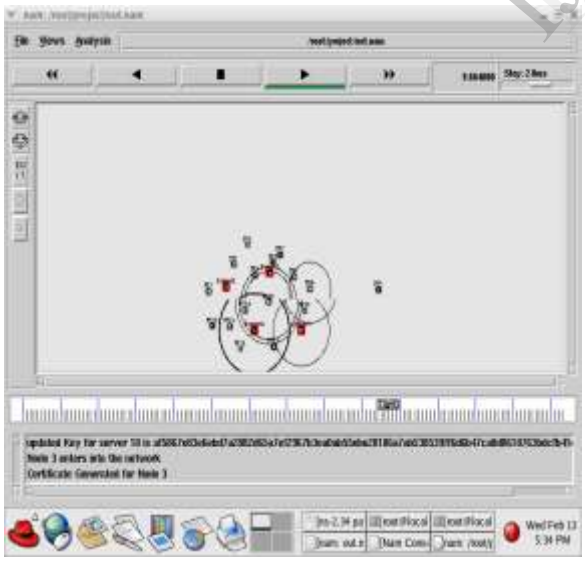

Figure 4: Certification Generation for Node3

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

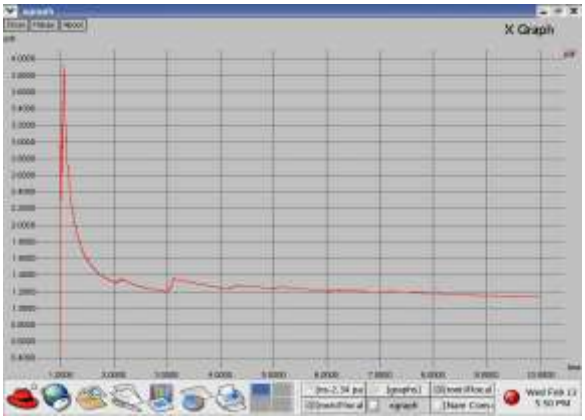

Figure 5: Packet delivery ratio

5 CONCLUSION

We form a typical deployment of sensor nodes with twenty numbers of nodes which are randomly deployed. The Message Digest5 Pure(MD5-Pure) and RSA algorithm is used to generate the certificate for the presented node. The other nodes are trustworthy at the time of deployment. Certificate is generated to the each node. The certificate contains the source address, destination address, public key, private key and the cipher text of actual data to be transmitted. 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. 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.

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, Member, IEEE, and Wensheng Zhang "Catching Packet Droppers and Modifiers in Wireless Sensor Networks" May 2012

[2] Mehdi Keshavarz, and Mehdi Dehghan, "MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks"

WCNC 2012 Workshop on 4G Mobile Radio Access Networks

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

[4] Leela Krishna Bysani Ashok Kumar Turuk "A Survey On Selective Forwarding Attack in Wireless Sensor Networks" February 2011

[5] Devika Bandyopadhya, Sangita Nath, D. Sheela, and Dr. G. Mahadevan **"**A Scalable Secured Approach in Wireless Sensor Networks**"** Aug-2011

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

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

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

[9] 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.

[10] 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

[11] 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.

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

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

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