Data Security in Wireless Sensor Networks to Improve Quality of Service

Anitha S
Professor, Department of ECE
ACS College of Engineering, Bangalore, India
(Affiliated to VTU, Belagavi)

Seelam Ch Vijaya Bhaskar
Asst.Prof, Department of IT
MVSR Engineering College, Hyderabad, India
(Affiliated to OU, Hyderabad)

Abstract – The current developments in Wireless Sensor Networks (WSN) woe from efficient and secure broadcasting of messages to a remote system. Even the communication is limited between group nodes and sender the secured transmission of data is difficult as there is no trusted public/private key generation center. To overcome these obstacles, this paper combines the broadcast encryption and group key management techniques to ensure data security using new cipher text generation methods. In this method each node maintains a single public/secret key pair, using which the remote sender broadcasts the message to the node by encoding the data with the group key. Even if the non-intended member collude they cannot extract information as the data is encrypted using the group key of the member. The group size is independent of computation and communication overhead which decreases the delay. Simulation results are presented using NS2.

Keywords – WSN, Network Lifetime, Public/Private Key, Group Key, Security, Throughput.

NOMENCLATURE
WSN: Wireless Sensor Network (WSN); PKI: Public Key Infrastructure (PKI)

I. INTRODUCTION

A WSN is an application specific multi-hop wireless networks consists of sensor nodes that operate on battery. The top layer in the WSN has the high speed internet entry points and the second layer consists of static routers which as the backbone to provide connection between each other via high speed, long range wireless methods. The bottom layer contains a large number of mobile network users. As the nodes in the WSN are grouped together to form a cluster and consists of open and distributed nature, it is difficult to provide security to the data. As the nodes collect the sensitive data, a malicious attacker or dropper can depict the data. The communication between a group to sender is challenging in WSN. The third party key generation centers cannot be fully trusted in these type of group communication. As the major security concern is with key management. Group key agreement protocol allows a set of users to negotiate on a single group key to encrypt and decrypt messages. This provides a better way to intragroup communication without completely depending on the central key management server. Various group key agreement protocols have been proposed in [2]-[13]. The earlier study [2]
[3] shows the building of efficient initial group key protocol. The later studies [4] provide efficient methods for member addition but the deletion of a member is still high. Tree structure proposed in [5] [7] [11] provides efficient methods to add or delete member nodes to a group. The theoretical analysis in [14] shows that in tree based group key agreement scheme the worst case cost for a member addition or deletion is computed as O(log n), where n is the number of group members. The proposed technique has the following aspects to provide secured group communication. Initially the problem is formalized for secured transmission for remote groups under certain conditions as the existing key management techniques does not provide optimal solutions. On the contrary group key agreement provides an optimal solution to secure communication within a group but, in case of a remote sender, it requires the sender to continuously communicate with the group members for repetitive rounds of interactions to share secret key before transmitting any sensitive information.

II. DESIGN ASPECTS TO IMPROVE QOS IN WSN

The nodes in WSN are application specific and are tightly coupled with the physical environment and provides distributed services. This differs the implementation of WSN from other wireless networks. The distributed services of the nodes are susceptible to various attacks. The proposed technique combines the broadcast encryption with group key agreement methods. Each group is given a public/shared key by the trusted third party key distribution system. When a sender is ready to transmit message to an intended group the message is encrypted using broadcast encryption and public/shared key of the group and it is broadcasted in the network. The non-intended cannot decrypt the message with their key. So in case of collusion data will not be lost and can be decrypted only by the intended group's public/shared key.

The members of a group can be added or deleted as follows, the sender can add a new member to a group by retrieving the public key of the user and inserting it to the public key chain of the current receiver set. Two receiver sets can be merged into single group by continually invoking the member addition operation. By continually invoking the member deletion operation, a sender can divide one receiver set into two sub groups by continually performing member deletion operation. The changes to the subsequent encryption and decryption procedures have to be updated after adding or removing a member.

Basic system model proposed:
This paper assumes that the network group is composed of N users i.e., $\{U_1, U_2 \ldots U_N\}$.

The scope of the paper is how efficiently and securely the transmission is possible from a sender to a subset of receivers S of N where n(S) <=N based on the following constraints.

i. In open networks like WSN it is difficult to design trusted senders and fully trusted key generation authority by all users.
ii. There is limited communication between the receivers to the sender, e.g. in the battlefield.
iii. The number of users N can be numerous like in vehicular networks.
iv. In the wireless communication as both the sender and the receiver sets are dynamic, according to the application scenarios, the following assumptions are made:
a. N can be any value less than 256.
b. The receivers cooperate and communicate with each other via efficient local channels.

To authenticate the receivers and the senders a Public Key Infrastructure (PKI) is available which can be partially trusted. Group key agreement based broadcast encryption can be used to address the problem of secured broadcast of data. The system architecture is illustrated in fig 1. Sensors are deployed around an area of interest and these sensor requires cooperative processing, which can be implemented by distributing sensor into groups. As the members in a group are less than the members in the whole network an intra group key pre distribution can be maintained. When a sender broad casts the data, it encrypts the data with the group key of the intended receiver. Each receiver has a public/secret key pair. The public key of each node is certified by key distributing authority and the private is kept with the node itself. Upon receiving an encrypted message each receiver decrypts is by applying its group key and its own secret key. In case of collusion data cannot be decrypted by non-intended sub group, which shows that receivers and senders need not communicate directly as data is encrypted using intra group communication. The sender can concurrently encrypt the message with the group key and only the designated receivers can decrypt. As shown in the following public/secret key generation algorithm.

Algorithms

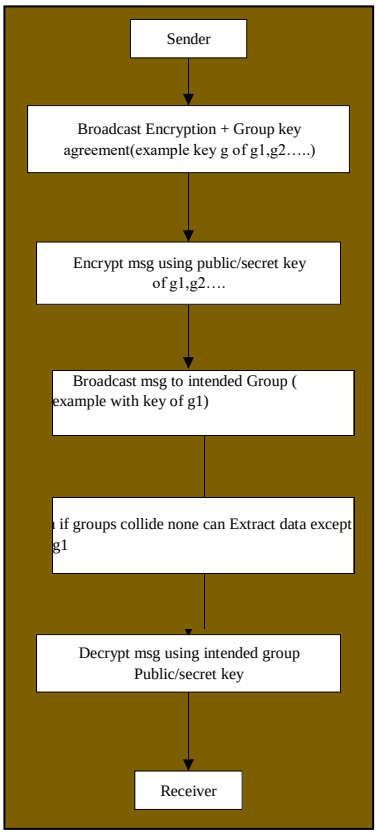

Fig 1. Encryption/Decryption

This is possible as public key infrastructures have been a standard component in many systems supporting security services.

1. Consider two different prime numbers s and t
2. Calculate the modulus n = s * t
3. Calculate the quotient $\tau(n) = (s - 1) * (t - 1)$
4. Select for public key an exponent which is integer k such that $1< k < \tau(n)$ and $\gcd(\tau(n), k) = 1$
5. Calculate for the private key exponent a value for j such that $j = k^{-1} \bmod \tau(n)$
6. Public Key = [k, n]
7. Private Key = [j, n]

Encryption: Let F be a file to be encrypted where the contents of F are taken into string S. Select random number r, where r <
m. Compute cipher text as: $c=g^{s\wedge k} \bmod n \times r^m \bmod m^2$.
Decryption: Compute original message using public/secret key of intended group. This method provides each receiver has a public/secret key pair.
The public key is of a node certified by a certificate authority, but the secret key is kept only by the receiver. When a sender needs to transmit data to a receiver, it receives the receiver's public key from key center and validates the authenticity of the receiver. To validate the receiver no direct communication is required between the sender and receiver.

S= (((c $^{\lambda}$ mod m^2 -1)/m) x μ mod m) ^{t} mod n Choose s = 7 and t = 13
Calculate n = s * t = 7 * 13 = 91
Calculate τ(n) = (s - 1) * (t - 1) = 6 * 12 = 72
Choose k such that 1 < k < τ (n) and k and n are co-prime. Let k = 3
Compute a value for j such that (j * k) % τ(n) = 1. One solution is j = 2 i.e., j= k−1 mod τ(n)
Public key is (k, n) => (3, 91) Private Key is (j, n) => (2, 91).

III. SIMULATION RESULTS & DISCUSSIONS

A sender can add a new member to a group by retrieving the public key of the member and inserting it to the public key chain of receiver set. By continuously invoking the member addition operation, a sender can merge two receiver sets into a single group. Figure 2 shows that each group in the network is given a group key which is used to encrypt the messages.

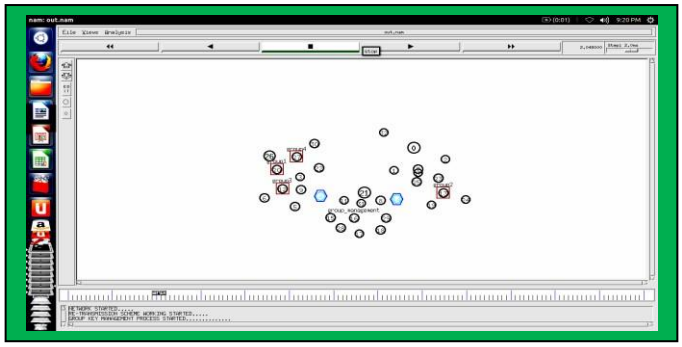

Fig 2. Start of group key management process

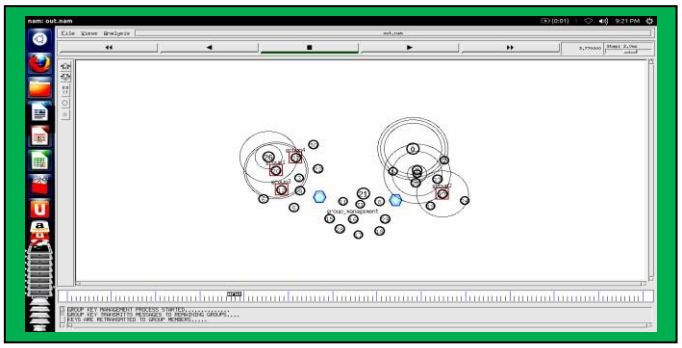

Fig 3. Keys are being transmitted among the groups

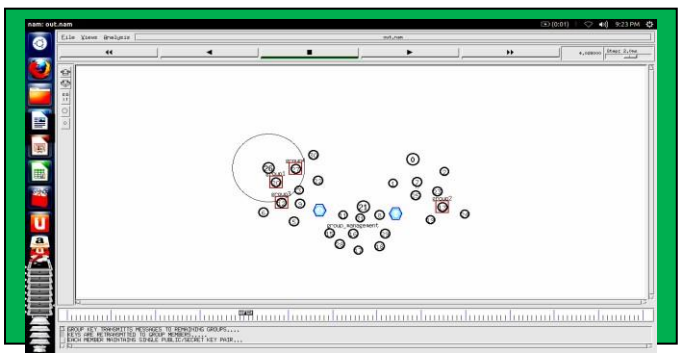

Fig 4. Now every member has the public and secret keypair

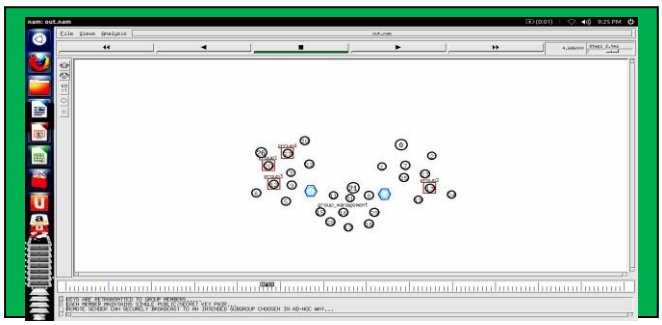

Fig 5. Remote sender sending messages only to the intended subgroup among the network

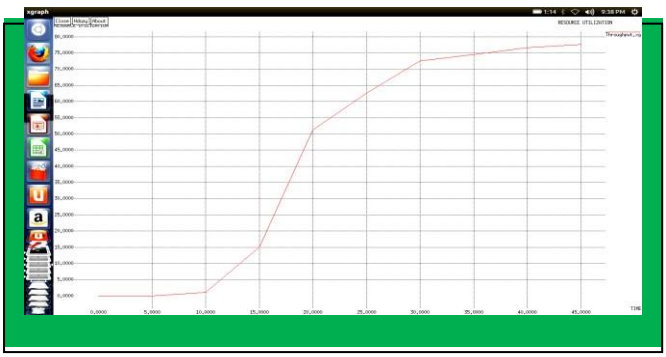

Fig 6. Resource utilization graph- indicates that as time progresses the network setup utilizes the maximum resources of the system

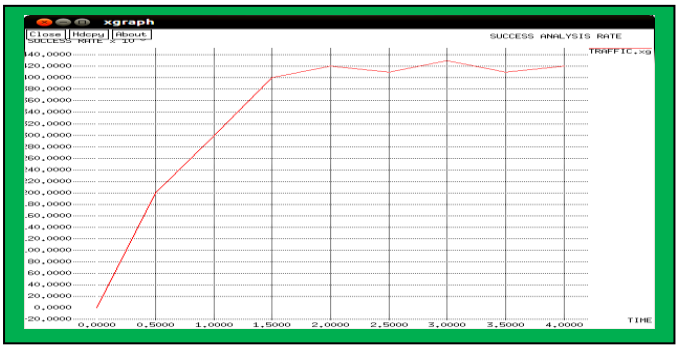

Fig 7. Success analysis rate graph which indicates that as the time progresses the more data is delivered at sender.

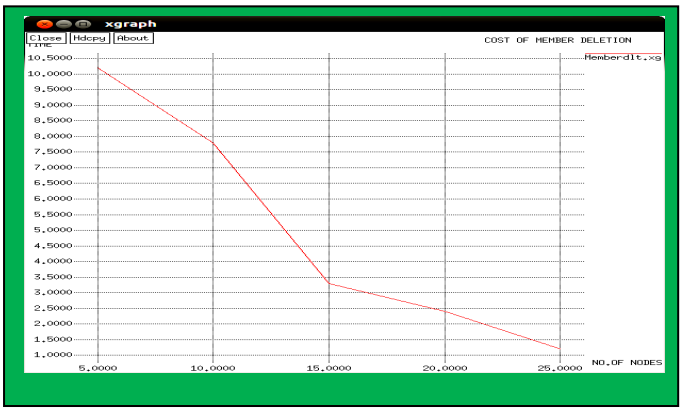

Fig 8. Cost of member deletion graph indicates that as the number of nodes increases the members has to bedeleted

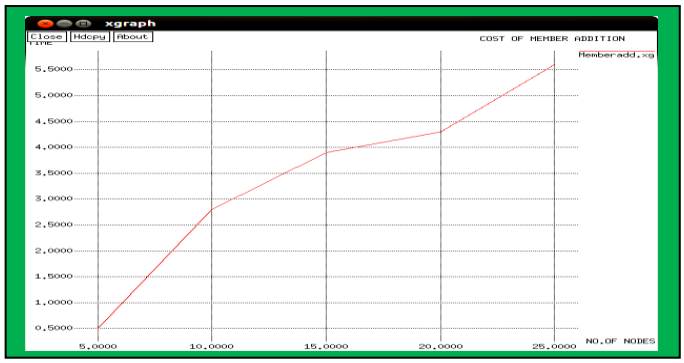

Fig 9. Cost of member addition graph indicates that as the time progresses depending upon the number of keys available members will be added to the sub-group

There are several applications that provides the security in the Wireless Sensor Network, that require service guarantees in order to function properly. These service guaranteed challenges are numerous, but the major challenge for traditional networks has been congestion and security. However, different QoS techniques are required for wireless networks over wired networks. In this paper the security in Wireless Sensor Network with cipher text is achieved.

The network constructed with 60 nodes which are divided into groups. The group key management process is depicted in figure 3 where each group is given public key, the public key is shared with other groups as shown in figure 4. Each group selects a private key as shown in figure 5 to encrypt and decrypt messages. A remote sender can send messages to the intended subgroup by applying its public key as shown in figure 6. Figure 7 and 8 shows the increase in resource utilization and data delivery rate as time increase. Figure 9 depicts the decrease in delay as the number of nodes deleted from the network and figure 10 shows the increase in time/delay as the number of nodes added to a subgroup.

IV. CONCLUSION

This paper provides the security in Wireless Sensor Network, the module are designed and implemented using NS2. The simulations are shows that this system provide the better security for WSN. This analysis gives the quality of the service in the Wireless Sensor Network is improved the better after seeing the results the QoS metric parameters are also taken into consideration for this analysis the proposed new key management system allows the sender to partially depend on the third party key generation center to ensure safe and secure broadcasting of data between sender and intended sub group. Collusions in the network cannot extract the data which enhances security. QoS is improved as the group size is independent of the computation and communication overhead, which decrease delay. This work can be further carried out by increasing the key size.

REFERENCES

[1] Qianhong Wu, Member, IEEE, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fellow, IEEE, and JesúsA. Manjón "Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm"- IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 2, APRIL 2013.

[2] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," Adv. Cryptol., vol. 950, EUROCRYPT'94, LNCS, pp. 275–286, 1995.

[3] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versakey framework: Versatile group key management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, pp. 1614–1631, Sep. 1999.

[4] M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769–780, Aug. 2000.

[5] Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444–458, May 2003.

[6] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure group communication using robust contributory key agreement," IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468–480, May 2004.

[7] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60–96, Feb. 2004.

[8] Y. Sun,W. Trappe, and K. J. R. Liu, "A scalablemulticast keymanagement scheme for heterogeneous wireless networks," IEEE/ACMTrans. Netw., vol. 12, no. 4, pp. 653–666, Aug. 2004.

[9] W.Trappe, Y.Wang, andK. J. R.Liu, "Resource-aware conference key establishment for heterogeneous networks," IEEE/ACM Trans. Netw.,vol. 13, no. 1, pp. 134–146, Feb. 2005.

[10] P. P. C. Lee, J. C. S. Lui, and D. K. Y. Yau, "Distributed collaborative key agreement and authentication protocols for dynamic peer groups," IEEE/ACM Trans. Netw., vol. 14, no. 2, pp. 263–276, Apr. 2006.

[11] Y. Mao, Y. Sun, M. Wu, and K. J. R. Liu, "JET: Dynamic join- exittree amortization and scheduling for contributory key management," IEEE/ACM Trans. Netw., vol. 14, no. 5, pp. 1128–1140, Oct. 2006.

[12] W. Yu, Y. Sun, and K. J. R. Liu, "Optimizing the rekeying cost for contributory group key agreement schemes," IEEE Trans. Depend. Secure Comput., vol. 4, no. 3, pp. 228–242, Jul.–Sep. 2007.

[13] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007–2025, May 2008

[14] J. Snoeyink, S. Suri, and G. Varghese, "A lower bound for multicast key distribution," Proc. IEEE INFOCOM, pp. 422– 431, 2001.