Secure Broadcast in Wireless Sensor Networks

A. Karthick kumar
Dept of Electronics and Communication Engineering
B.s.Abdur rahman university
Vandalur,Chennai-48
Kumar.akarthick783@gmail.com

Mrs. G. Anuradha
Dept of Electronics and Communication Engineering
B.s Abdur rahman university
Vandalur,Chennai-48
Anuradha@bsau.ac.in

***Abstract*— Authenticated broadcast is enabled from base station to low powered sensor nodes using tesla family schemes. In existing µ-TESLA scheme the performance is decreased at packet loss and delay time .The proposed x-TESLA scheme overcomes these problems. The x-TESLA broadcast authentication scheme can resist the problems and leads to efficient solutions to the problems.**

***Index Terms*— Security, broadcast authentication, wireless sensor networks.**

I. INTRODUCTION

Authentication and security are the core challenge in wireless sensor networks. Due to the sensitive nature of the data gathered by many wireless sensor networks (WSNs) it is becoming critical that this data be protected. However, due to the constrained nature of the resources available on sensor nodes, traditional wireless networking security solutions are not viable due to their processing requirements, speed and communications overhead. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges .The advancement in wireless communications and integration of electronics technology have enabled the development of low cost, low-power, multifunctional sensor nodes. The most important is the security aspect in Wireless Sensor Network. In order to provide an effective integrity, confidentiality, authentication during communication, the need of Security issues emerges in Wireless Sensor Network.
From base station to sensor nodes the security is essential to avoid the malfunctions When constructing the sensor network, authentication is necessary for many administrative tasks
Traditional techniques of security will give the new challenges. that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. The tesla broadcast authentication sechme in distributed networks is important in wireless sensor networks [1].Efficient security authentication and security mechanism in wirless sensor networks[3],[5].The security and authentication in wireless sensor networks in [11].The authentication code verification. After verification of key of message authentication code the receive will receive ,otherwise the receiver will discard the packets. The X-TESLA broadcast optimized broadcast in wirless sensor networks in [12].The TESLA is the secure broadcast authentication scheme in wireless sensor networks. Timed efficient stream loss authentication is security mechanism for efficient security in wireless sensor networks. The µ-TESLA based on loose time synchronization. In µ-tesla broadcast authentication scheme the message authentication code(MAC) is used. The message authentication code is based on the symmetric key techniques. The broadcast authentication of µ-tesla from base station to sensor nodes with key management. The sender will attach the message authentication code with packets and send to the receiver. The receiver will receive the packet until the message authentication code verification. After verification of key of message authentication code the receive will receive otherwise the receiver will discard the packets. The X-TESLA broadcast authentication scheme is the another scheme for wirless sensor networks for efficient packet delivery in wirless sensor networks. The x-tesla broadcast authentication scheme uses the technique called cross authentication scheme. The repeated authentication is increase the security efficiency.

II. PROBLEMS

A. *Packet loss*

After verification of MAC the receiver will receive the packets during the sleep mode of the sensor nodes heavy computation will performed. Thus the heavy packet lose will occur. Limited buffering required for the sender and the receiver, and therefore timely authentication for each individual packet.

B. *Delay time*

The delay time of the node and computation will leads to packet losses. The delay of nodes is depends upon the node of key delivery of each node from sender to receiver. The delay of node is described in seconds in the graph.

III. OVERVIEW OF µ- TESLA

The existing µ-TESLA broadcast authentication scheme is based on the TESLA security mechanism. The µ-tesla is based on the secret key based cryptographic operation are needed to authenticate a broadcast message. The original TESLA uses broadcast to distribute the initial parameters is guaranteed by a digital signature generated by the sender. The authenticity of the parameters the base station and sensor nodes are loosely time syncronised.

The µ-TESLA security scheme uses symmetric key techniques. A sender broadcast a message with a message authentication code generated with a secret key, which will be disclosed certain period of time. When a receiver receives this message, if it can ensure that the packet was sent before the key was disclosed, the receiver can buffer this packet and authenticate it when it receives the corresponding disclosed key. To authenticate the broadcast messages ,a receiver first authenticates the disclosed keys. The sender prefers a long delay in order to make sure that all or most of the receivers can receive its broadcast messages. But ,for the receiver , a long delay could result in high storage overhead to buffer the messages.

The µ-tesla uses a security condition to prevent a receiver from accepting any broadcast packet authenticated with a disclosed key. when it receives the corresponding disclosed key to The sender will send the message with message authentication code(MAC) key to receiver ,if the key matches the receiver will receive.

A. *The multilevel-µ tesla*

In single chain µ-tesla broadcast authentication scheme having no practical limit. In multilevel µ-tesla scheme uses multiple chain for broadcast authentication .In multi level chain during long interval time of messages the Dos –attacks should be described.we can use the large node to steore the messages.

The other technique is hash function to resist the Dos-attacks in multilevel µ-tesla based on the tesla security broadcast authentication scheme. The simple scheme can greatly reduce the overhead involved in distribution of key chain commitments in µ-tesla because unicast –based message transmission is not required any more. The life time of sensor network is divided into long interval of duration .The high-level key chain has pseudo random function. The duration of the high-level time intervals is usually very long compared with the network delay and clock discrepancies.

IV. THE ALGORITHM

The Algorithm is based on the two tables. The first table hellman table for precomputation. The next table is online phase. The hellman table is used in online phase.

A. *hellman table creation*

In hellman table the number of chain and chain length are described. The P is nontrivial permutation is the 64-bit value and defined $\hat{H}=P°H$.

Algorithm 1. Create Hellman table T

1. Open an empty table T
2. for $0 \le i < m$ do
3. Choose random 64-bit value x.
4. $y \leftarrow x$
5. for $0 \le j < t$ do
6. $y \leftarrow H(y)$
7. end for
8. Add ordered pair (x, y) to T
9. end for
10. Sort T according to the second components

The hellman table is based on the m table entries and one time sorting m elements.. This table generating key for messages. And the table predict the key chain and chain length.

B. online phase table creation

In online phase table is used for invert H value in hellman table .

Algorithm 2.Invert H = F

Require: Hellman table T created by Algorithm 1

1. InvCtr ←0
2. for every $y \in D$ do
3. $y' \leftarrow P(y)$
4. for $0 \le i < t$ do
5. if $(x; y') \in T$ for some x' then

6. x← x'

7. for 0 ≤ j < t - i -1 do

8. x ←H (x)

9. end for

10. if H (x)= P(y) then

11. print "x maps to y under H."

12. InvCtr← InvCtr + 1

13. else

14. print "False alarm." (optional)

15. end if

16. end if

17. y' ←H (y)

18. end for

19. end for

20. print "InvCtr keys inverted." (optional)

The online phase table will uses a false alarm sheme for key verificatation. The key management is used for false alarm scheme.

V. X-TESLA OVERVIEW

The x-tesla broadcast authentication scheme is based on the cross authentication of multiple chains of upper level and lower level. The x-tesla is based on the loosely time syncronised between base station and sensor nodes. The packet loss, sleep modes will be avoided by repeated authentication.

The proposed x-tesla the time is divided into intervals for lower level chain and upper level chain. The message authentication and acceptance based on the security condition.

The x-tesla broadcast authentication scheme will decrease the packet loss and delay time and more efficient the existing systems. In x-tesla broadcast authentication scheme uses the cross authentication scheme. The cross authentication scheme uses the upper level and lower level chain management scheme for repeated authentication for more security performance.

A. Cross *authentication scheme*

The cross authentication scheme will uses the upper level and lower level chain for authentication scheme.

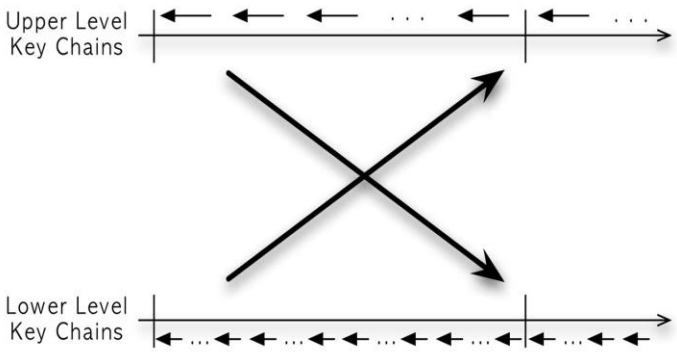

Fig 1. Cross authentication

The x-TESLA cross authentication scheme is based on the flow of upper chain and lower chain authentication. The number of unauthenticated packets and disclosure of key is based on the interval in x-tesla scheme.

B. *Implementation of algorithm*

The implementation of µ-tesla and x-tesla scheme is in network simulator. The algorithm implementation in network simulator is based on the nodes and performance of packet loss and delay time of the nodes. The security implementation is based on the secret key in every node and performance is measured.

C. *Packet loss comparison*

The packet loss comparison berween µ-tesla and x-tesla shows the authentication of packet delivery from base station to sensor nodes. The relialbility of authentication is performed well in x-tesla.

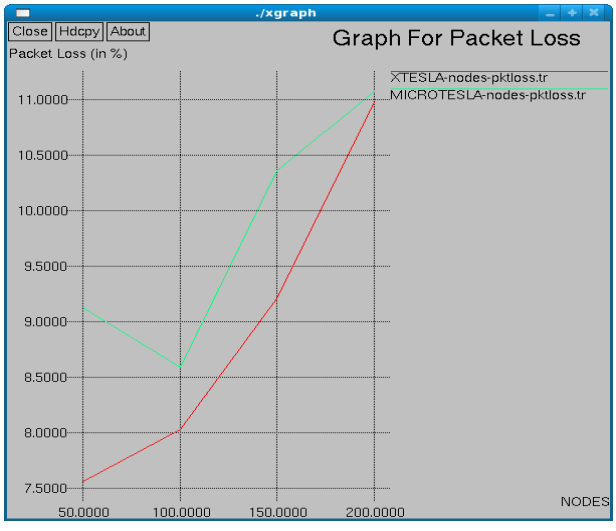

Fig.2 Packet loss

The authentication is more efficient in x-tesla and avoiding packets loss.

D. *End to end delay*

The key delivery from base station to sensor nodes the delay is very effective in x-tesla broadcast authentication scheme.

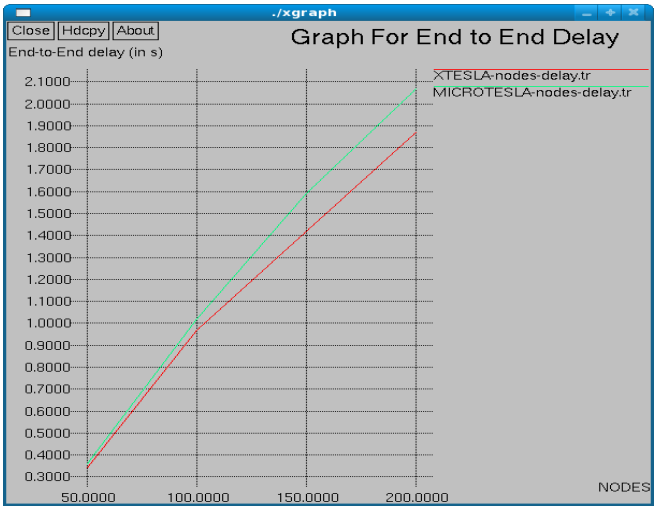

Fig. 3 Delay time of nodes

The delay time of the node is very effective in x-tesla scheme when compared to µ-tesla broadcast authentication scheme.

VI. CONCLUSION

The x-tesla broadcast authentication scheme is very efficient when compared to µ-tesla broadcast authentication scheme. The packet loss and life time of the nodes are very effective in x-tesla scheme. The delay time of the nodes are low when compared to µ-tesla broadcast authentication scheme.

REFERENCE

[1] D. Liu and P. Ning, "Multi-Level _TESLA: Broadcast Authentication for Distributed Sensor Networks," ACM Trans. Embedded Computing Systems, vol. 3, no. 4, pp. 800-836, Nov. 2004

[2] M. Luk, A. Perrig, and B. Willock, "Seven Cardinal Properties Sensor Network Broadcast Authentication," Proc. ACM Workshop of Ad Hoc and Sensor Networks (SASN), Oct. 2006.

[3 A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. ISOC Network and Distributed System Security Symp. (NDSS), Feb. 2001.

[4]. W. Ye, J. Heidemann, and D. Estrin, "Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks, "IEEE/ACM Trans. Networking, vol. 12, no. 3, pp. 493-506, June 2004

[5]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 62-72, 2003.

[6]. D.J. Malan, M. Welsh, and M.D. Smith, "A Public-key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. And Network, Oct. 2004.

[7.] A. Durresi, V. Paruchuri, S. Iyengar, and R. Kannan "Optimized Broadcast Protocol for Sensor Networks," IEEE TrannsComputers vol. 54, no. 8, pp. 1013-1024, Aug. 2005.

[8]. Q. Li and D. Rus, "Global Clock Synchronization in Sensor Networks," IEEE Trans. Computers, vol. 55, no. 2, pp. 214-226, Feb. 2006.

[9] G. Avoine, P. Junod, and P. Oechslin, "Time-Memory Trade Offs: False Alarm Detection Using Checkpoints," Proc. Indocrypt '05, pp. 183-196, 2005

[10]. A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57, June 2004.

[11]. A. Durresi, V. Paruchuri, S. Iyengar, and R. Kannan, "Optimize Broadcast Protocol for Sensor Networks," IEEE Trans. Computers,vol. 54, no. 8, pp. 1013-1024, Aug. 2005.

[12] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." Proc. ACM Conf. Computer and Comm . Security (CCS), pp. 62-72, 2003.

[13] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "TinySeRSync: Secure and Resilient Time Synchronization in Wireless Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS), 2006.

[14] K. Kar, A. Krishnamurthy, and N. Jaggi, "Dynamic Node Activation in Networks of Rechargeable Sensors," IEEE/ACM Trans. Networking, vol. 14, no. 1, pp. 15-25, Feb. 2006.

[15] J.Dj. Goli_c, "Cryptanalysis of Alleged A5 Stream Cipher," Proc. Eurocrypt '97, pp. 239-255, 1997.