International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

Secure Dynamic Program Update Protocol for ZigBee Using ECC

Vishwa pratap singh[1], Divya Pal Singh[1], Ashwini Saini[2]
ABV-Indian Institute of Information Technology and Management[1]
Morena link road, Gwalior, M.P., India
Department of Computer Science, Kurukshetra University, Kurukshetra[2]

***Abstract*— Wireless sensor networks are very low power network, comprises of several sensor nodes have low computational power and very limited storage. The nodes employed in hostile environment and generally unattended, they can be easily compromised and keys stored in nodes can be retrieved. We have proposed a new secure low power consumption scheme ,dynamic program updates protocol for ZigBee using ECC, on compromised sensor nodes .We also identify the shortcoming in paper -Security Weakness in a Dynamic Program Update Protocol for Wireless Sensor Networks by Peng Zeng, Zhenfu Cao,Kim-Kwang Raymond Choo, and ShengbaoWang . We eliminate their shortcomings in our paper.**

Keywords —Wireless sensor networks, dynamic program Update, security, ECC,

I. Introduction

Low power sensor networks[1] comprised of several distributed sensor nodes, which have very low computation power ,very less memory and run on battery .Sensor nodes are deployed in an area to monitor several environmental phenomena like humidity, temperate, pressure ,vibrations, light and physical Phenomena like pollutant gases, motion of certain size items etc .IEEE 802.15.4[2] is the basis for ZigBee and specifies the protocol and compatible interconnection for data communication devices using low-data-rate, low-power and low complexity, short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN).ZigBee[3] is a suite of high level communication protocols for connecting small, low power digital radios, wide variety of low power sensor nodes and regulated by Zigbee Alliance.

ZigBee nodes are spread in wide area and have certain programs Installed in them. Nodes work according to the installed programs. Time to time programs installed in sensor nodes need to be updated , new security patches have to install according to our need ,as nodes are spread in wide area and thousands in number so it is very time consuming and tedious task to update each node manually. Nodes are deployed in hostile and harsh environment and mostly remain unattended and susceptible to many security threats. Data from the sensor nodes can be easily retrieved. Updating programs present in nodes dynamically is a major concern. ZigBee comes in two flavors ZigBee and ZigBee Pro, ZigBee pro is more secured version. ZigBee Pro[4] uses public and private key cryptography and define three types of keys[9] , link key, master key and network key. Whole of security depends on these three keys .If attacker get successful in capturing the node and retrieved all keys from that node; whole of the security architecture will fail. We cannot use public and private key cryptography based on keys in dynamic program updating as nodes can be easily captured and cryptographic keys present in sensor nodes can be easily retrieved. We are proposing scheme based on ECC[7] to update program in captured ZigBee node dynamically. Our scheme updates ZigBee nodes unlimited number of times without concerning about cryptographic keys. In recent years many algorithm for dynamic updating have been proposed and mostly are based on public and private key cryptography and digital signature[10]. But if node gets compromised and attacker is able to retrieved cryptographic keys, whole of the scenario will fail.

II. Related Work

In 2008 Das and Joshi[5] present protocols for dynamically updating sensor nodes using orthogonality[8] principle but there are many flaws in their algorithm. All security in their algorithm depends on the parameter old needs to be reinstalled on all sensor nodes before deploying them in the field, and old must be dynamically updated by all sensor nodes whenever they accept a correct advertisement message. Thus, old acts as a dynamic secret key shared by the base station and all sensor nodes in the Das-Joshi scheme. This is, however, a design flaw as if attacker is able to compromised WSN node and get old. Attacker can successfully impersonate the base station to broadcast its own update[4].

To overcome security flaws in Das and Joshi scheme, Peng Zeng,Zhenfu Cao [6] had proposed a new algorithm based on orthogonality principle. Their scheme able to update WSN node in secure manner on compromised WSN node, Their scheme have two weaknesses first is limited number updates. They have taken Euclidean space V of dimension n and, after a singular value decomposition analysis, decompose V into two orthogonal subspaces V1 of dimension k and V2 of dimension n-k. The base station randomly selects an orthogonal basis of V1, O1,O2, E ,O ,k, and a vector Ci ,V2 for each sensor node i. The orthonormal basis is known only to the base station. The vector Ci are installed node i before deploying it in the field. The numbers of updates are depending on the subspaces V1 . V1 is calculated using K, the number of updates is limited to K only. After K updates node have to be manually configured to update WSN node in secure manner. Second weakness is in acknowledgement. There is only one way communication. Server will never know about node is securely updated or not.

III. The Proposed Scheme

In this section we present our proposed scheme to removes the weaknesses present in previous schemes. Our scheme has two phases. In setup phase all calculation and installation programs done before deploying ZigBee node in the field. In Dynamic updating phase base station sends the update to all ZigBee nodes. Zigbee nodes get the update, authenticate it and update program installed in it.

TABEL 1
NOTATION USED IN PROPOSED SCEME

*	additive multiplication of points over elliptic curve
h	one way hash function
M	program
$M^{adv}_{(j)}$	advertisement send by base station
X^{pid}	program id
X^{ver}	program version
t_j	time of sending advertisement
j	advertisement number

A. *Assumptions*

- All ZigBee nodes are full function device, which is able to send and receive data.
- Base station is fully secured and has very high computation power and large storage.
- Attacker can get the data stored in the node but cannot change the stored data in Zigbee node.

B. *Setup Phase*

Before deploying the ZigBee node in the field we have to install α_1 , β_1 and hash function in the ZigBee node. First of all we install hash function in the node then carry out following steps on base station to calculate α_1 , β_1.

Step 1: Base station chooses an elliptic curve over GF(2^n) with n should be very large.

Step 2: Base station choose a point $e_1(x_1, y_1)$ on chosen elliptic curve.

Step 3: Base station choose a random number *d* (using pseudo random number generator).

Step 4: Base station calculate hash of d to get D_1 using SHA.

Step 5: Base station calculate

$$e_2(x_2, y_2) = D_1 * e_1(x_1, y_1)$$

Multiplication above is multiple additions of points in GF (2^n)[11]

Step 6: Let consider points

$$e_1(x_1, y_1) \text{ as } \alpha_1$$

$$e_2(x_2, y_2) \text{ as } \beta_1$$

Step 7: Install α_1 , β_1 in the Zigbee node.

Step 8: Deploy the ZigBee node in the field.

C. *Dynamic node update phase*

When base station want to send update to Zigbee node, following steps are carried out at server side.

Step 1: Base station calculates $e_3(x_3, y_3)$, $e_4(x_4, y_4)$ and D_2 in same manner as setup phase.

Step 2: Base station calculate hash of

$$(j , t_j , M, X^{pid} , X^{ver} , D_1 ,\beta_2,\alpha_2)$$

Step 3: Base station keep *D2* to itself and send update $M^{adv}_{(j)}$ to all nodes.

$$M^{adv}_{(j)} =[(j , t_j , M, X^{pid} , X^{ver} , D_1 ,\beta_2,\alpha_2), h(j , t_j , M, X^{pid} , X^{ver} , D_1 ,\beta_2,\alpha_2)]$$

At node side

ZigBee node receive the adv $M^{adv}_{(j)}$ and carry out following steps.

Step 1: Node calculate hash of

$$(j , t_j , M, X^{pid} , X^{ver} , D_1 ,\beta_2,\alpha_2)$$

using hash function installed in r node and compare with hash

$$h(j , t_j , M, X^{pid} , X^{ver} , D_1 ,\beta_2,\alpha_2)$$

stored in $M^{adv}_{(j)}$ to check the integrity of the $M^{adv}_{(j)}$. If the calculated hash is equal to the stored hash move to second step, otherwise discard the $M^{adv}_{(j)}$.

Step 2: Validate t_j with the local current time *Clock*. If the inequations

$$/ Clock - t_j / < \triangle t$$

Holds, then proceed to next step, else reject the message. Here $\triangle$t denotes the time of the expected network delay which can be estimated according to different applications.

Step 3: Calculate β_1 using the α_1 preinstalled in node and D_1 extracted from the $M^{adv}_{(j)}$,

$$\beta_1 = e_2(x_2, y_2) =D_1 * e_1(x_1, y_1)$$

If calculated β_1 is equal to the installed β_1 in node move to next step otherwise discard advertisement.

Step 4: Install the program M in the node and replace the new α_2 and β_2 with preinstalled α_1, β_1 in the node.

Step 5: Reply the base station with J, X^{pid} , X^{ver}.

IV. SECURITY ANALYSIS

A. Update Authentication

Security in scheme lies in calculating D_1 with known α_1 and β_1. Attacker can retrieve α_1 and β_1 from Zigbee node.Attacker must have tofind a multiplier(D_1) that creates β_1 starting from point α_1.Calculating D_1 is an elliptic curve discrete logarithmic problem[12].This problem can only be solved by Polard rho algorithm,which is infeasible if n and D in GF(2^n) is large.Proposed scheme authenticate update with D installed in it,and if attacker is not able to find D in any mean then our scheme is secure.

B. Replay attack

For each update scheme replace α_{n+1} and β_{n+1} with α_n, β_n and changing D attacker never able to replay previous updates.

C. Update delay attack

ZigBee node calculate time delay using

$$|\text{Clock} - t_j| < \triangle t$$

if the delay is more than $\triangle t$ ZigBee node discard the update.

D.Unlimited Number of Updates

ZigBee nodes can be updated unlimited number of times as for each update base station calculate new α, β and D. α , β and D can be calculated any number of times.

V. CONCLUSION

We have removed the one weaknesses present in Peng Zeng, Zhenfu Cao as only limited numbers of updates are possible. we have presented a scheme which is able to update ZigBee node unlimited number of times in unsecured environment and restricted WSN. Secured acknowledgements of update by ZigBee node remain as future work.

References

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol.40, no.8, pp. 102-114, August 2002.

[2] Gutierrez, J.A. and Naeve, M. and Callaway, E. and Bourgeois, M. and Mitter, V. and Heile, B, “IEEE 802.15. 4: a developing standard for low-power low-cost wireless personal area networks,” Network, IEEE, vol. 15,no.15, pp.12–19,2001.

[3] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006).pp1-203,2007

[4] Radmand, P. and Domingo, M. and Singh, J. and Arnedo, J. and Talevski, A. and Petersen, S. and Carlsen, S., “ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys,” P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on,pp.465-470,2010.

[5] Manik Lal Das and Aakash Joshi’’ Dynamic Program Update in Wireless Sensor Networks Using Orthogonality Principle’’ *in IEEE COMMUNICATIONS LETTERS, VOL. 12, NO. 6, pp 478-481,2008..*

[6] Peng Zeng, Zhenfu Cao, Kim-Kwang Raymond Choo, and Shengbao Wang’’ Security Weakness in a Dynamic Program Update Protocol for Wireless Sensor Networks’’ *IEEE COMMUNICATIONS LETTERS, VOL. 13, NO.* 6, JUNE 2009.

[7] 8.Vanstone, S.A. ; Zuccherato, R.J. “Elliptic curve cryptosystems using curves of smooth order over the ring Zn’’ Information Theory , *IEEE Transactions on july 1997,page number 1231-1237,1997.*

[8] Sayed , A.”orthogonality principle "*Book Adaptive filters press ,Wiley IEEE press page number* 67-77.

[9] ZigBee, PRO,” Specification, 2007”, San Ramon, California: ZigBee Alliance (October 2007),2007.

[10] S. Lee, H. Kim, and K. Chung, “Hash-based secure sensor network programming method without public key cryptography,” in *Proc. the Workshop on World-Sensor-Web at International Conference on Embedded Networked Sensor Systems*, 2006.

[11] Deschamps, J.-P. and Sutter, G..,” Elliptic-Curve Point-Multiplication over GF(2^{163}),” Programmable Logic, 2008 4th Southern Conference on.pp.25-30,march 2008.

[12] Smart, N.P.,” The discrete logarithm problem on elliptic curves of trace one,” Journal of cryptology,vol.12.no.3.pp.193-196,1999.