A Novel Key Pre-distribution for Wireless Sensor Networks

A.M.Bharath Kumar[1],Ashok Kumar Balijepalli[2]
[1]Asst.Professor,Dept of ECE,Krishna chaitanya Inistitute of Technology and Scince, Markapur,Prakasam(Dist),Ap,India.
[2] Asst.professor, Department of ECE,Guntur Engineering College,Yanamadala,Guntur(Dist),Ap,India..

***Abstract*— To establish the two key in wireless sensor network is a basic security services, forming the basis other security services, such as authentication and encrypted. However, due to the sensor network resource constraints on to establish the two key not wireless sensor networks trivial tasks. The existing key, pre-alpha-ever scheme compromise node number and a minor part however influence key will increase quickly. As a result, a small compromise the number of node may affect the most adversaries. This paper proposes an improved key management wireless sensor network plan, take advantage of one-way hash function to alleviate the influence of compromise the sensor high sensor nodes. At the same time, this method does not affect the connection between neighbouring sensor node. The analysis shows that compared with the existing plan which has good network resilience against node capture attack.**

Keywords*— *Key Pre-distribution; wireless sensor networks; security services

Introduction

Wireless sensor network is composed of a large number the sensor nodes through converging wider area connections, and have different kinds of applications include environmental monitoring, industrial monitoring, safety, security services, military system, the medical service, etc. These mission critical applications in wireless sensor network make security and privacy of function requirement. However, in wireless sensor networks achieve security is a challenging because the task, particular constraint ability understanding sensor node (battery supply, CPU, memory, etc) and stern deployment of a sensor network. A safe and key performing encryption and authentication must reach agreement by transportation node. However, due to the resources constraint network of sensors in much key agreement mechanism used in general networks, and other public key to not feasible scheme Sensor network. There are three types of key management scheme in has been studied wireless sensor networks: trust, server solution, scheme and key pre-distribution, get enforcing scheme. Reliable server solution of dependence trust key distribution server and management [1, 2]. This type of scheme is not verbs forFig.1: Security Implementation Technique in WSNs.

wireless sensor networks because usually lack of trust infrastructure application environment, wireless sensor networks use. Get enforcing scheme, on the other hand, with asymmetric encryption, for example, key distribution management use public-key certificate. However, limited company calculation and energy resources usually sensor nodes make it undesirable use public key algorithms, such as RSA. To save energy the second type of the key management solutions, namely, the key pre-alpha-ever plan, such a plan pre-alpha-distributed key information scheme seems the most appropriate wireless sensor network; it is types of scheme we think here. Two straight forward solutions can distribute symmetric-key to wireless sensor node. The first solution is to make all the sensor nodes storing a same master key [3]. Any two nodes can use this global master key realization agreement and acquired new double key. Although these look verbs are simple and effective system has good effectiveness, this scheme does not exhibition desirable network elasticity. If a node is damaged, safety of the whole wireless sensor, the network will be compromised. Some existing research shows. In temper - resistant storage master key hardware reduced Risk [4], but this increased costs and energy consumption. In addition, resistant hardware tamper don't always safe [5]. At the other extreme, some may consider giving each pair of sensor nodes region double key. This means that each sensor nodes need to store n-1 different double key in its memory if have n node to wireless networks sensor network. This solution has the perfection of network security because any sensor node of capture or compromise will not affect non-begin the communication between the nodes. This plan is main limitation key is stored in his head, this makes it is not suitable for large wireless sensor network. In recent years many pre-distribution applicable key scheme has proposed establishing double key. In literature [6] [7]

[8] [9] [10] [12] [11] [13], the existing key pre-distribution scheme, number of number compromise node, increased rates of influence double key increases rapidly. Therefore, a small part compromise node may lead to substantial double key damage.

Related work

The first key puts forward pre-alpha-ever Eschenauer and Gligor in [5], and was assigned sensor nodes random subset from a big key in key pool deployment of the network. Deployment after two adjacent, however, can build sensor nodes between them the key as long as they had at least one common feature in their key rings. Unfortunately, such key pools are very susceptible to in collusion. A few attackercontrolled node. Headquarters in this scheme, Chen, Perrig, and song [7] put forward a q-composite random key pre-alpha-ever scheme, increase safe key settings, the attacker must more compromise nodes to achieve a high possible possibilities communication. The difference between the composite programs and solutions [6] requirements, this scheme at least asked (q : 1), not just a single one common keys, two sensor node, establish a shared key. These ask keys are the hash into a key and achieve better elasticity sensor node capture. The quantity that you need to share the keys index is difficult; the attacker to consider the key links given already damaged part of the key. Improve security of two random schemes key space [9, 12] have been proposed. An applicable key pre-distribution for sharing mechanism is to establish sensor network. Liu Sun Li puts forward [10] gather rather similar double key scheme based on the key distribution scheme [12]. In these two kinds of schemes, much key space precompiled and each sensor associated with one or more key space before deployment. Two sensor nodes can be calculated a double key deployed if they have keying information from an ordinary key space. In the two solutions, the communication between non-begin sensor node keep a safe compromise of sensor nodes quantity less than a critical value. But once the critical value is too big, the opponent will collapse all double key. To have good scalability, a use knowledge base key management presents [13]. In this deployment point, the proposed multiple definitions each sensor network deployment point, a key space pre-computed. Neighboring deployment points a number key in common. All of the sensor node before classification deployment, each group corresponds a deployment point. Each sensor randomly selected from core several keys space group. Sensor nodes deployed, after closing has a high probability of neighborhood sharing a common key. The scheme has a strong demand, but deployment has good expansibility and those proposals [7] [8] [9] [10]. Overall structure to establish the two key in wireless sensor networks is studied in [14], is based in baled polynomial-key pre-alphaever agreement [12] proposes.

The proposed scheme

In this section, we present our proposed double key establish plan in detail. In the most crucial predistribution scheme, communication between pair wise key sensor node key memory cards used is not directly [6, 7], or can be from secret pre-loaded stock [9, 10, 11, 12]. Then once sensor nodes are captured and opponent might crack other sensor nodes and even whole network through compromise keys or secret stocks. According to this problem, the program all keys hash value key pool formation a new key pool. What we call the key is in key hash value derivative key be caused by. Because one-way hash function the nature, anyone can easily derived from the original keys, but nobody calculated from the original keys.

Key Predistribuion

This phase is done offline mainly by key distributed server (KDS) before deploying sensor node to the target area. It is the following steps:

Step 1: KDS produce very big scale of key pool, and identify different keys. KDS assigns each key an unique ID.

Step 2: KDS hash value calculates the key use the same pool hash function H and store it in these cheap key pools. here, we use these hash value derivative key be caused by. Now the key pool has two seconds keys, an half the original keys and derivative keys. Step 3: For each sensor node, KDS storage hash function H, it used to create derivative key into each sensor node.

Step 4: For each sensor node, KDS random selection of key from the core pool S and store them into each sensor node. Here, we call it a set of t key nodes keys. In this scheme, we think derivative k the same key id and original key k.

Shared Key Discovery Phase

After sensor nodes have been deployed, shared key discovery phase will be implemented. In this phase, the sensor for the first time that key nodes is discovery. Their neighbors share a key. Detect whether a node there is a common characteristic ID front have its neighbors and source node disclosure of the key documents and type of list these keys destination node. Hypothesis sensor u and sensor v. Neighbors gained

the key list and the type of intrusion detection systems (IDs). If they decided they have common features identifier. They can be calculated pair wise key. As follows:

Example 1: Below this kind of circumstance, common keys are used as their double key. That is if they are original key, double. The key is that the original key ko , if they are derived the key is caused by the derivative key adversary.

Example 2: The key sensors are you a completely original key, the key sensor v derivatives of the key. In this case, the double key is derivative Kd and sensor I need calculation opposite be caused by calculate H (ko).

Path Key Establishment

The critical path used to assign establishment stage however sensor node to a nearby key, do not share common keys, being connected two or more links to create. The key findings in the Shared phase. Des can get new double key from this message. If direct key establish sensor network node failed, the two can try to establish an adversary key critical path establishment stage. When a source sensor radio ID of sensor, a destination Intermediate sensor may formulate a path of key two ff can pair wise source sensor nodes and with the sensor destination, respectively. Otherwise, intermediate sensor broadcast message constantly until find share sensor pair wise keys with previous sensor and destination sensor etc. The path of key can build along the message broadcast path in the reverse direction.

Performance analysis

In this section, we evaluate the network security property proposed method and make suggestions and then compare the proposed scheme with several existing key pre-distribution scheme.

Establish Direct Key

Now we calculate the local connection computer, the probability the sensor two adjacent establish communication double key directly. Similar to the analysis in [6], the two nodes probability have the same key id. This is sensor node two probability to establish direct key.

$$p_c = 1 - \frac{\left\{ \begin{matrix} 2s \\ t \end{matrix} \right\} \left\{ \begin{matrix} 2s-2t \\ t \end{matrix} \right\}}{\left\{ \begin{matrix} 2s \\ t \end{matrix} \right\} \left\{ \begin{matrix} 2s \\ t \end{matrix} \right\}}$$

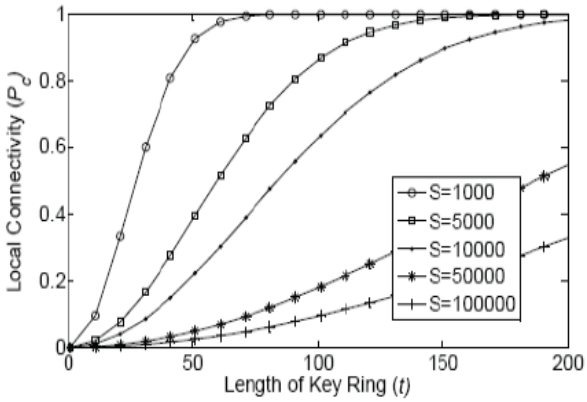

Fig. 1 Probability of establishing direct keys between neighbor sensor nodes for different *S*

Figure 1 shows the probability to establish direct key different number of key preload, each sensor. From this find we can see with the same key S and pool size. Key ring lengths are not local connected to the scheme.

Resilience against sensor capture

Node capture attacks the most serious threats wireless sensor networks, an adversary may body be trapped Sensor node secret information storage compromise, after have one Wireless sensor nodes are not compressive due to its low cost. Random key pre-alpha-ever plan [6, 7], the same key can be sensor network different photoes, some sensor capture may affect communication and other non-captured node. Here, the tough measurement schemes by forecasting short total network communication, so the occupation X node does not include communication compromise of nodes are directly involved. In this section, we studied the scheme of elastic of sensor capture through the probability analysis.

$$P_b = 1 - \left\{ 1 - \frac{3t}{4s} \right\}^x$$

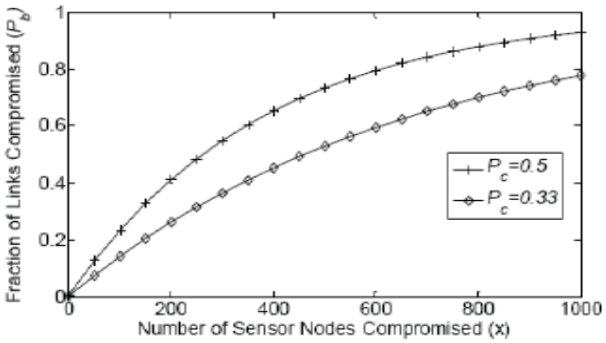

Fig. 2 Fraction of compromised link between non-compromised nodes, after an adversary has compromised *x* random nodes

Figure 2 includes a fraction of the relationship between them the damaged links, non-begin nodes and number of compromise node. We could see more the sensor compromise, higher scores links, non-begin to compromise.

Comparision with other scheme

Assess our work, in this section we compare previous work plan. Safety mainly comparison in here, this is non-begin a fraction of influence. Here, we chose Eschenauer-Gligor scheme [6], q-composite Plan (q=2, 3) [7], [8] because DDHV scheme compared with our plan.

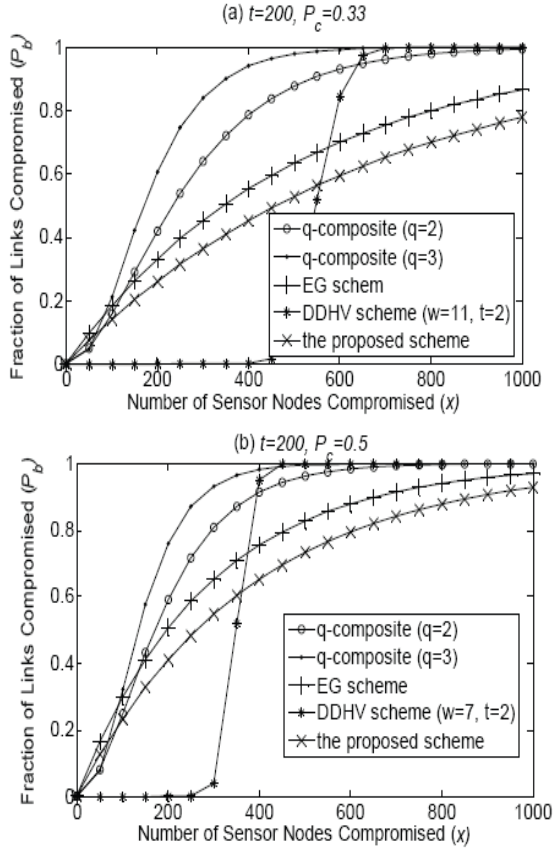

Fig. 3 Fraction of compromised link between non-compromised nodes, after an adversary has compromised *x* random nodes.

Figure of links between comparative compromise scores non-begin sensor obtain the same place connected PL, T and storage overhead. We can see that our plan obviously better than the other three schemes. For example, Give PL = 0.33, there are 500 sensor nodes is damaged, There will be a 63 percent of the link. Non-compromised between compromise Sensors in such as solution, in q-composite 84% (q = 2), in q-composite 96% (q = 3), it is only 50% in our plan. Although when DDHV proposal execution pair wise key than our plans are established. Some sensor network node, the opponent will control compromise the entire network once number of compromise sensors node than threshold.

Conclusion

We presents a pair wise key management plan wireless sensor networks, some damaged sensor node only affect the sensor node uncompromising part and one-way hash function, this scheme can make the attacker get less critical information from the damaged sensor node. We have conducted a study of connectedness. The results show that the proposed scheme is considerable elastic reason for the opposition Sensor nodes are caught.

References

[1] A. Perrig, R. Szewczyk, J.D. Tygar, et al. SPINS: Security protocols for sensor networks. Wireless Networks, 2002, 8(5): 521~534

[2] H. Chan, A. Perrig, D. Song. Key distribution techniques for sensor networks. Wireless Networks, 2004, 6(2): 277~303

[3] C. Karlof, N. Sastry, D. Wagner TinySec. TinySec: A link layer security architecture for wireless sensor networks. in: Proc. of 2nd Int. Conf. Embedded Networked Sensory Systems. New York, NY, USA: Association for Computing Machinery, 2004. 162~175

[4] L. Bocheng, K. Sungha. Scalable session key construction protocol for wireless sensor networks. Embedded Systems, 2002, 2(2): 58~71

[5] R. Anderson, M.Kuhn. "Tamper resistance –A cautionary note", Proc. Of the 2nd USENIX Workshop on Electronic Commerce , 1996.1~11

[6] L. Eschenaure and V.D. Gligor, "A key-management scheme for distributed sensor networks". in: Proc. of the 9the ACM Conference on Computer and Communications, Washington DC, USA, pp.41-47, Nov. 2002

[7] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks", in: Proc. 20003 IEEE Symposium on Security and Privacy, pp.197-313, May 2003

[8] W.Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution schemes for sensor networks networks". ACM Transactions on Information and System Security, Vol.8. No2,May(2005)228-258

[9] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks". ACM Transactions on Information and System Security, vol.8, pp.41-77, Feb. 2005

[10] R. Blom, "An optimal class of symmetric key generation systems. Advance in Cryptography". London, UK: Springer- Verlag, pp.335-338 , 1985

[11] C. Blundo, A. D. Santis, A. Herzberg. S. Jutten, U. Vaccaro, and M. Yung. "Perfectly secure key distribution for dynamic conference", Information and Computation, vol.1, pp.1-23 , Jan. 1995

[12] W.Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution schemes for sensor networks networks using deployment knowledge". IEEE INFOCOM , pp597, 2004

[13] D.Liu and P.Ning, "Location-Based pairwise key establishment for static sensor networks", Proc. 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp.72-82, 2003