Fast Energy-Efficient Secure Dynamic Address Routing For Scalable WSNs

Mr. G. Ravi[1], Mr. M. Mohamed Surputheen[2] & Dr. R. Srinivasan[3]

[1]Research Scholar, Dr.M.G.R Educational and Research Institute University, Chennai, India

[2]Research Scholar, Dr.M.G.R Educational and Research Institute University, Chennai, India

[3]Research Supervisor, Dr.M.G.R Educational and Research Institute University, Chennai, India

Abstract

Secure Routing is one of the important issues in wireless sensor networks. A number of approaches have been proposed for secure routing in wireless sensor networks, but there is a lack of sufficient support for quick &secure routing in large-scale sensor networks. We consider the dynamic address routing for wireless sensor networks. We consider two security algorithms namely RSA (Rivest, Shamir &Adleman), Elliptic Curve Cryptography (ECC) as an initial test for dynamic address routing protocol for wireless sensor networks. We consider five routing attacks such as Directory attack, Brutal attack, Wormhole attack, Sinkhole attack and Sybil attack against dynamic address routing in wireless sensor networks. In this paper, we propose a common key cryptographic security algorithm named Random Number Addressing Cryptography (RAC) for providing energy efficient secure dynamic address routing protocol for scalable wireless sensor networks. RAC security algorithm works energy-efficiently and provides better security than RSA and ECC.

Keywords: *Sensor Networks, Secure Routing, Dynamic Address Routing, Security Algorithms and Common Key Cryptography*

1. Introduction

Our focus is on dynamic routing security in wireless sensor networks. The current proposal for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application of specific nature of the networks, but do not give much emphasis on security. Security in wireless sensor networks are currently provided through public key cryptography such as RSA and ECC. It is widely believed that the complexity cost of public-key algorithms make them unsuitable for resource constrained applications. The proposed RAC cryptographic algorithm provides efficient encryption of data and enhances security.

The contribution of this paper includes attacks on sensor networks routing and security algorithms. Section 1.1 gives the detailed information about the Dynamic Address Routing (DART) Section1.2 gives the various attacks on sensor routing in detail. Section 2 gives the information about security algorithms RSA and ECC.Section 3 gives the detailed information about the proposed security algorithm RAC.

1.1 Dynamic Address Routing

It is well known that the current ad hoc routing protocol suites do not scale to work efficiently in networks of more than a few hundred nodes. Those routing protocols use static addressing which leads to a massive overhead problem in sensor networks as the number of nodes grow. The main idea behind DART is to separate node's address and identity. DART satisfies the following properties which can be seen as guidelines for a scalable and efficient solution:

- Localization of overhead
- Lightweight, decentralized control
- Zero configuration
- Minimal restriction on hardware

Using dynamic addressing and appropriate routing, DART [2] is a promising approach for achieving scalable routing in large wireless sensor networks.

1.2 Routing Attacks in Sensor Networks

The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the message.

1.2.1 Directory attack

In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or pass phrase by searching likely possibilities. A dictionary attack uses a targeted technique of successively trying all the words in an exhaustive list called a dictionary (from a pre-arranged list of values). In contrast with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities, which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phrase dictionary attack) or a bible etc. Generally, dictionary attacks succeed because many people have a tendency to choose passwords that are short (7 characters or fewer), single words found in dictionaries or simple, easily predicted variations on words, such as appending a digit in the passphrase.

In general it can be defined as a method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password. A dictionary attack consists of trying “every word in the dictionary” as a possible password for an encrypted message. A dictionary attack is generally more efficient than a brute force attack if the user choose poor passwords. Dictionary attacks are generally far less successful against systems that use pass phrases instead of passwords. If an extensive dictionary attack fails, it may be worthwhile to resort to a brute force attack. A brute force attack is more certain to achieve results eventually than a dictionary attack.

1.2.2 Brute Force attack

In cryptography, a brute force attack or exhaustive key search is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make his/her task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space.During this type of attack, the attacker is trying to bypass security mechanisms while having minimal knowledge about them. Using one or more accessible methods: dictionary attack (with or without mutations), brute-force attack (with given classes of characters e.g.: alphanumerical, special, case (in) sensitive) the attacker is trying to achieve his/her goal. Considering a given method, number of tries, efficiency of the system, which conducts the attack and estimated efficiency of the system, which is attacked, the attacker, is able to calculate how long the attack will have to last. Non-brute force attacks, on the other hand, which include all classes of characters, give no certainty of success.

2.3 Wormhole attack

The Wormhole attack [3], usually needs two malicious nodes. The idea is to distort routing with the use of low-latency out-bound channel to another part of the network where messages are replayed. These can be used, for example, to create sinkholes and to exploit race conditions.

1.2.4 Sinkhole attack

In a sinkhole attack [4] the adversary’s goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the packets follow have many opportunities to tamper with the application data, sinkhole attacks can many other attacks (selective forwarding, for example). Sinkhole attacks typically work by making compromised node look especially attractive to surrounding nodes with respect to the routing.

1.2.5 Sybil attack

In a Sybil attack [5], is targeted to undermine the distributed solutions that rely on multiple nodes cooperation or multiple routes. In a Sybil attack, the malicious node gathers several identities for posing as a group of many nodes instead of one. This attack is not relevant as a routing attack; it can be used against any crypto schemes that divide the trust between multiple parties. For example, to break a threshold crypto scheme one needs several shares of shared secret.

2. Security Algorithms

The security algorithms are actually used to detect, prevent and recover from the security attacks. The

RSA and ECC security algorithms are considered for secure routing in wireless sensor networks. These two security algorithms provide less security than RAC and e RAC.

2.1 Rivest, Shamir & Adleman (RSA)

The RSA security algorithm is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n. A typical size of n is 1024 bits, or 309 decimal digits. That is, n is less than 2^1024. Plain text is encrypted in blocks with each block having a binary value less than some number n. That is the block size must be less than or equal to log2 (n). In practice the block size is I bits, where 2^i <n<=2^(i+2). Encryption and decryption are of the following form, for some plaintext block M and cipher text block C.

$$C = \lambda\ f' \bmod \eta$$
$$M = c^0 \bmod \eta = (\lambda'' \bmod \eta = \lambda\ f^{-1} \bmod \eta)$$

Both sender and receiver must know the value of n. the sender knows the value of e and only the receiver knows the value of d. Thus this is a public key encryption algorithm with a public key of PU = {e,n} and a private key of PR ={d,n}. For, this algorithm to be satisfactory, the following requirements must be met:

1. It is possible to find the values of e, d, n such that M^ed mod n =M for all M<n.
2. It is relatively easy to calculate M^ed mod n and C^d mod n for all values of M<n.
3. It is infeasible to determine d given e and n.

The following procedure states the RSA scheme. The ingredients are the following:

P, Q two prime numbers (private, chosen)
n=p q (public, calculated)
e, with gcd (ϕ(n),e)=1;1<e<ϕ(n) (public, chosen)
$d=e^1 \pmod{\phi(n)}$ (private, calculated)

The private key consists of {d,n} and the public key consists of {e,n}. Suppose that user A has published its public key and that user B wishes to send the message M to A. Then B calculates $C = \lambda\ f' \bmod \eta$ and transmits C. On receipt of this cipher text, user A decrypts by calculating $(M=c^0 \bmod n)$

2.2 Elliptic Curve Cryptography (ECC)

The addition operation in ECC is the counterpart of the modular multiplication in RSA and multiple additions are the counterpart of modular exponentiation. To form a cryptographic system using elliptical curves, we need to find a hard problem corresponding to factoring the product of two primes or taking the discrete algorithm.

Consider the equation Q=kP where Q, P Є E_F (a,b) and k<p. It is relatively easy to calculate Q given k and p, but it is relatively hard to determine k given Q and P. This is called the discrete logarithm problem for the elliptical curves.

The task is to encode the plaintext message m to be sent as an x-y point P_m. It is the point P_m that will be encrypted as a cipher text and subsequently decrypted. We cannot simply encode the message as the x or y co-ordinate of a point, because not all such coordinates are in E_a(a,b).

As with the key encryption system, an encryption/decryption system requires a point G and an elliptical group E_a (a,b) as parameters. Each user A selects a private key η_A and generates a public key $P_\lambda\ \eta_{A\ oG}$

To encrypt and send a message P_m to B. A chooses a random positive integer k and produces the cipher text c_m consisting of the pair of points:

$$c_{m\ \{\lambda'\ 'G.}\ P_m\ |\lambda'\ P_S\}$$

3. Proposed Security Algorithm

This section describes the proposed common key cryptographic security algorithm RAC for secure routing in wireless sensor networks. The RAC principles are explained with the references [6, 7]

3.1 RAC (Random number-Addressing Cryptography)

We have exploited the innovative cryptographic streaming of data that is the continuous encryption or decryption of data [8, 9].The cryptographic streaming named RAC does not complicate operations at all, but automatically scrambles memory access at hardware level. RAC is a common key technique with ideal cipher strength like Vernam cipher.

This is because it directly encrypts full plain text without division. RAC is really practical in view of actual implementation. RAC is theoretically high speed, because it does not do any arithmetic logic operations like XOR, but simply does memory access. It is possible to implement RAC security algorithm for secure routing in wireless sensor networks.

3.2 RAC Algorithm

1) Main Block

Step:1 Specify the data scanning mode, Store and Initialize the data in buffer
Step:2 Go to Address Generation Block and generate the transposition addresses
Step:3 Do Encryption or Decryption with Transposition Block
Step:4 Do Step:1-3 until the end of buffer and last scan

2) Address Generation Block

Step:1 Read the initial value
Step:2 Random Number Generator
Read the sequence
Generate a random number; assign it to the members of the sequence
Do until the end of sequence
Step:3 Return the transposition addresses

3) Transposition Block

Step:1 Read the $[n]^{th}$ content of the buffer
Step:2 Write into the Random$[n]^{th}$ address of the Buffer
Step:3 Do until the end of the content
Step:4 Return the encrypted/decrypted content

Conclusion

Good cryptographic implementations are essential in wireless sensor networks if the secure routing of the communications is to be assured. As wireless sensor networks technologies begin to be incorporated into applications on a large scale, the secure encryption of data in routing is becoming more vital.

We proposed security algorithm RAC is consumed less power with more security level. We conclude that it is possible to implement these security algorithms for routing very effectively on resource-constrained platform such as wireless sensor networks.

References

[1] Gerad Murphy, Aiden KeeshanRachit Agarwal Emanuel Popovici, "Hardware –Software Implementation of Public-Key Cryptography for Wireless Sensor Network" in IEE Irish Signals Systems Conference, June 28-30, 2006.

[2] J. Erickson, M.Faloutos and Srikanth V. Krishnamurthy , " DART : DynamicAddress RouTing forScalable Ad Hoc and Mesh Networks"in IEEE/ACMTransactions on Networking, Vol15, No 1, February 2007.

[3] Y-C. HU. A. Perrig, and D.B Johnson, Wormhole detection in wireless and ad hoc Networks. Technical report, Department of Computer Science, Rice University,December 2001 Technical Report TR01-384

[4] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and Countermeasures, Elsevier's Ad Hoc Networks Journal, Special issues on Sensornetworks Applications and Protocols, 1(2-3);September 2003, 293-315.

[5] J. Douceur, The sybil attack, In Proceedings of the IPTPS 2002, Cambridge, MA,USA, March 2002.

[6] M. Fukase and T. Oyama and Z. Liu "Endeavor in the field of Ranom Sampling- Designing and Prototyping a Processor Suited for its Application", Technical Report of IEICE, vol. 102, no. 272. 2002, pp. 7-12.

[7] M. Fukase, and T.Sato, "Power Concious Endeavor in Processors to Speed Up Random Sampling:,Poc. Of SCI2003, vol. V, 2003, PP. 111-116.

[8] M.Fukase, A.Fukase ,Y.Sato, and T.Sato "Cryptographic System by a Random Addressing – accelerated Multimedia Mobile processor ," Proc of SCI2004, vol II,Jul. 2004, pp. 174-179.

[9] M.Fukase, A.Fukase, Y.Sato, and T.Sato, "Exploting a Hardware Security-EmbeddedMultimedia Mobile Processor System and its Application," ITC-CSCC, 2004, pp.7C3L-3-1-7C3l-3-4.

First Author: G.Ravi, Master of Computer Applications-1987, M.Phil Computer Science-1996; Associate Professor & Head in Computer Science, Jamal Mohamed College at Tiruchirappalli, India; has presented several papers in National Conference & participated in International Workshop on his field of Research; his current Research includes Neural Networks, Computer Networks, Wireless Sensor Networks and Network Management.

Second Author: M.Mohamed Surputheen M.Sc Mathematics-1986, M.Phil Computer Science-1996; Associate Professor in Computer Science, Jamal Mohamed College at Tiruchirappalli, India; has presented several papers in National Conference & participated in International Workshop on his field of Research; his current Research includes Genetic Algorithms, Computer Networks, Network Management and Wireless Sensor Networks.

Third Author: Dr.R.Srinivasan, M.Sc Physics, University of Madras-1960, M.S Electrical Engineering University of Hawaii, USA-1970, D. Sc Electrical Engineering Washington University, St. Louis, USA-1974, In R& D: 35 years (1960-95)in National Aerospace Laboratories, Bangalore, in R & D Projects & also as Head, Computer Centre - Design & Development of Data Logging Systems for Wind Tunnel Instrumentation and also Management of Large Computer Centre, Member of NAL's Parallel Processor Flosolver Laboratory. Currently he is working as Dean R&D and PG Studies and Professor, Computer Science Department, RNS Institute of Technology, Bangalore, India