Oriental Journal of Computer Science & Technology Vol. **3**(2), 299-304 (2010)

Key management with cryptography

SYED MINHAJ ALI[1], SATISH V REVE[1], ROOHI ALI[2*] and SANA IQBAL[3]

[1]Department of Computer Science & Engineering, RGPV University, Bhopal (India).
[2]Department of MCA, GGGC, RGPV University, Bhopal (India).
[3]Department of Computers, Saifia Science College, Bhopal - 462 001,(India).

(Received: August 12, 2010; Accepted: September 04, 2010)

ABSTRACT

In this paper, we present an idea of adopting certificateless public key encryption (CL-PKE) schemes over mobile ad hoc network (MANET), which has not been explored before. In current literature, essentially there exists two main approaches, namely the public key cryptography and identity-based(ID-based)cryptography .Unfortunately, they both have some inherent drawbacks. In the public key cryptography system, a certificate authority (CA) is required to issue certificates between users' public keys and private key stoen sure their authenticity, whilst in an ID-based cryptography system, users' private keys are generated by a key generation center (KGC), which means the KGC knows every users' keys (the key escrow problem). To avoid these obstacles, Al-Riyami and Paterson proposed certificateless cryptography systems where the public keys do not need to be certified and the KGC does not know users' keys. Essentially, certificateless cryptography relies between the public key cryptography and ID-based cryptography. In this work, we adopt this system's advantage over MANET .To implement CL-PKE over MANET and to make it practical ,we incorporate the idea of Shamir's secret sharing scheme.The master secret keys are shared among some or all the MANET nodes.This makes the system self-organized once the network has been initiated. In order to provide more flexibility, we consider both a full distribution system and a partial distribution system. Furthermore, we carry out two simulations to support our schemes. We firstly simulate our scheme to calculate our encryption, decryption and key distribution efficiency. Then we also simulate our scheme with AODV to test the network efficiency.The simulations are performed over OPNET.

Key words*:* certificateless cryptography, MANET, AODV, OPNET, public key cryptography, identity based cryptography, secret sharing.

INTRODUCTION

Growing number of business operations conducted via Internet or using a network environment for exchanging private messages requires increasing means for providing security and privacy of communication acts. Cryptography techniques are essential component of any secure communication.Two main cryptography systems are used today: symmetric systems called also systems with a secret key,and public-key systems. An extensive overview of currently known or emerging cryptography techniques used in both type of systems can be found in [121. One of such a promising cryptography techniques is applying cellular automata(CAs).CAs were proposed for public-key cryptosystems by Guan[1] and Kari[5]. In such systems two keys are required: one key is used for encryption and the other for decryption, and one of them is held in private, the other rendered public. The main concern of this paper are however cryptosystems with a secret key. In such systems the encryption key and the decryption key are the same. The encryption process is based on generation of pseudorandom bit sequences, and CAs can be effectively used for this purpose.CAs for systems with a secrete key were first studied by Wolfram[16], and later by Habutsu *et al.*[3], Nandietal.

[IO] and Gutowitz[2]. Recently they were a subjectof study by Tomassini & Perrenoud[141], and Tomassini &Sipper[151] who considered one and two dimensional (2D) CAs for encryption scheme. This paper is an extension of these recent studies and concerns of application of one di- mensional (ID) CAs for the secret key cryptography.The paper is organized as follows. The next section presents the idea of an encryption process based on Vernam cipher and used in CA-based secret key crypto system.Section 3 outlines the main concepts of CAs, overviews current state of applications of CAs in secret key cryptography and states the problem considered in the paper. Section4 outlines evolutionary technique called cellular programming and section 5 shows how this technique is used to discover new CA rules suitable for encryption process. Section6 contains the analysis of results and the last section concludes the paper

Mobile Ad Hoc Network

MANET Overview : Mobile Ad-hoc Network

(MANET) is one of the most widely discussed and researchedareas in the field of wireless communications.In a traditional network, mobile devices connect toeach other via an access point. If the access pointfails, users cannot communicate to each other. In theMANET scenario, no access point or node is required.MANET is a network that only consists of mobile2devices such as personal digital assistants (PDAs)and laptops. It requires no centralized infrastructurelike basic switch centers or wireless routers. Nodesconnect to each other via the ad hoc model. Nodeswork not only as a host but also as a router, joiningor leaving the network at any moment, making thenetwork highly dynamic.

Because of MANET's non-centralized infrastructure and highly dynamic characteristics, routing is an essentialpart of this network. Without routing, devicesare unable to connect to each other, and the networkbecomes crippled. Routing protocols for the Internetdo not perform very well in MANET. Routes may becomeinvalid at any second, which may be caused bya slight movement of one node. In this case, dynamicadaptive routing protocols must be applied.AODV Ad-hoc on-demand distance vector (AODV)routing protocol is an on-demand routing protocol inMANET proposed by Perkins, Belding-Royer and Das[10, 7]. In this protocol, nodes do not perform routinguntil a request is generated or received. It uses threetypes of control messages: Route Request (RREQ),Route Reply (RREP) and Route Error (RERR) to controlthe whole network.

In order to discover a Destination Node (DN), the source node (SN) broadcasts a RREQ message. A sequencenumber is given to each node which has receiveda RREQ message. When this RREQ message finds itsway to the DN, a RREP message is generated, sendingback to the SN the same way the RREQ came from,and thus a route is established. After this, this route will be assigned with a lifetime. Every time a messageis transferred via this route, the lifetime is refreshed.When the lifetime is expired, the route becomes invalid.

Existing Key Management Schemes

Partially distributed authority scheme Partially distributed authority scheme was firstly Proposed by Zhou and Hass[8]. In their scheme it is assume that there is an Offline Trust Third Party (OTTP) constructing and distributing keys for all the nodes. Firstly, this OTTP generates a pair of master public/ secret keys. The master public key (mpk) is known by every node in the MANET, while the master secret key (msk) is divided into n parts, where each part is presented by $Si(i = 0, 1, 2...n)$. Then OTTP picks n arbitrary nodes, randomly distributed with msk parts.

These n nodes collectively form the Distributed Certificate Authority (DCA).The OTTP then generates certificates for all of thenodes and distributes them respectively. In Zhou andHass' scheme, those certificates are fully stored in each DCA node as well.This provides authentication from potential threads of unauthorized nodes. Any unauthorized node does not have valid certificate, thus will not get key shares from DCA nodes. Assuming the threshold of the system is t, node I needs to obtain at least t+1 m sk shares to retrieve them sk. Node i will send out requests to t DCA nodes, with a certificate of its own. Once the certificate is verified by a DCA node, which is achieved by comparing with DCA's certificate database, the DCA node will reply with a share of msk. After successfully obtain valid key shares, node *i* will retrieve the msk.This brings an imbalanced load to the DCA nodes ,because those DCA nodes are in charge of the whole network. This scheme also requires pre-establishment before the initiation. Certificates of each node are pre stored in the DCA nodes.In order to solve these problems, Yi and Kravers proposeda modified model[6]. It makes use of the broadcast certification request (CREQ) and the certification reply (CREP) packets. It allows nodes to broadcast the certification request (CREQ) packets using a flooding method. Any DCA which gets this packet answers with a certification reply (CREP). If the node successfully collects *t*+1 CREPs, it will be able to reconstruct thefull certificate. If the certificate is valid, the certification is successful; otherwise, the node will generate another CREQ packet.

Issues and design principles

We incorporate a distributed system to replace the KGC, so that the network becomes self-organized. This fully distributed system is based on the threshold cryptography with two patterns (*t, n*). The pattern *t* represents the threshold of the model, which means any*t+1* malicious users can break the system (hence, the system is upper bounded by *t*+1, which means that as long as there are at most *t* malicious users, then the system is considered to be at the 'secure' state). The pattern *n* represents the total number of users. We denote *n'* to be the maximum number of users, and 'to be the number of malicious users in the network at the initiation state. *t'* should be less than *t* to get the network initiated. Unfortunately, we cannot anticipate if a new-joint node is malicious or not. If the system is based on fully distributed model, then in the worst case, all the new-joint nodes are malicious, which add up to *n'-n+t* 'malicious DKGC nodes. In order to keep the system running well, this *n'-n+t'* should be smaller than *t*. The system becomes vulnerable when *t-t'* nodes join the network. If the system is based on the partially distributed model, every DKGC sends its data to a random non DKGC node before it goes offline. When *t-t'* original nodes goes offline, and they all replicate themselves to new-joint node, the system becomes vulnerable. Fully distributed systems are more efficient, but only allow a small number of new-joint nodes. Partially distributed system can be secure as long as certain amount of origin nodes stay online, but it requires cooperation between DKGC nodes and new-joint nodes,and it brings along with extra communication overhead searching for DKGC nodes. Different systems should be chosen over different scenarios.

Vernam Cipher and Secret Key Cryptography

Let P be a plain-text message consisting of m bits PIP~...P~, and ki&...& be a bit stream of a key k. Let ci be the i - th bit of a cipher-text obtained with use of XOR(exclusive-or) enciphering operation:

The original bit pi of a message can be recovered by applying the same operation XOR on ci with use of the same bit stream key k: The enciphering algorithm called the Vernam cipher is known to be [8, 121 perfectly save if the key stream is truly unpredictable and used only one time. From practical point of view it means that one must find answers on the following questions: (a) how to provide a pure randomness of a key bit stream and unpredictability of random bits, (b) how to obtain such a key with a length enough to encrypt practical amounts of data, and (c) how to pass safely the key from the sender to receiver and protect the key.In this paper we address questions (a) and (b). We will apply CAs to generate high quality pseudorandom numbe rsequences (PNSs) and a safe secret key. CAs has been used successfully to generate PNSs. We will show that the quality of PNSs for secret key cryptography and a safety of the key can be increased with use of ID CAs.3 Cellular Automata and Cryptography One dimensional CA is in a simpliest case a collection of two-state elementary automata arranged in a lattice of the length N, and locally interacted in a discrete time t. For each cell i called a central cell, a neighborhood of a radius r is defined, consisting of ni = 2r + 1 cells, including the cell i. When considering a finite size of CAs a cyclic boundary condition is applied, resulting in a circle grid. It is assumed that a state cl:+' of a cell i at the time t + 1 depends only on states of its neighborhood at the time t, i.e. qi1 +1 = fkLLQ,ll, d2, "'> &), and a transition function f, called a rule, which defines a rule of updating a cell i. A length L of a rule and a number of neighborhood states for a binary uniform CAs is L = 2", where n = ni is a number of cells of a given neighborhood, and a number of such rules can be expressed as 2L. For CAs with e.g. r = 2 the length of a rule is equal to L = 32, and a number of such rules is 2a2 and grows very fast with L. When the same rule is applied to update cells of CAs, such CAs are called uniform CAs, in opposite to non uniform CAs when different rules are assigned to cells and used to update them. The first who applied CAs to generate PNSs was S. Wolfram[161]. He used uniform, ID CAs with r = 1, and rule 30. Hortensius *et al.,*[4] and Nandi et al. [IO] used nonuniform CAs with two rules 90 and 150, and it was found thatthe quality of generated PNSs was better that the qualityof the Wolfram system. Recently Tomassini and Perrenoud[14] proposed to use non uniform, ID CAs with r = 1 and four rules 90, 105, 150 and 165, which provide high quality PNSs and a huge space of possible secret keys which is difficult for cryptanalysis. Instead to design rules for CAs they used evolutionary technique called cellular programming(CP) to search for them.In this study we continue this line of research. We will use finite, ID, non uniform CAs. However, we extend the potential space of rules by consideration of two sizes of rule neighborhood, namely neighborhood of radius r = 1 and r = 2. To discover appropriate rules in this huge space of rules we will use CP.

Classical cryptography(CC)

'Security through computational complexity' is the working rule for Classical Cryptography. It uses one way mathematical operations which makes the reverse process of finding the key or plain text an almost impossible job. But if eve is assumed to have infinite computational power, then CC backslides bringing around a disadvantage into this field. Briefing on a Couple of CC Algorithms

Public Key Cryptography

In 1976, Whitfield Diffie and Martin Hellman changed theparadigm of cryptography forever They used twodifferent keys, one public and the other private. It iscomputationally hard to deduce the private key from thepublic key. Anyone with the public key can encrypt amessage but not decrypt it. Only the person with the privatekey can decrypt the message. It is as if someone turned thecryptographic safe into a mailbox. Putting mail in themailbox is analogous to encrypting with the public key; anyone can do it. But opening the mailbox (a strong vault) and reading the content is easier for the one with the key rather than the one with a hacksaw. There are many algorithms which use this concept but the most popular andcogent one is the RSA Algorithm. RSA Algorithm with example:

1. Choose two prime numbers (p, q)
   E.g. $p = 61$ and $q = 53$
2. Compute $n = pq$: n = 61 x 53 = 3233
3. Compute the totient $\Phi(n) = (p-1)(q-1)$
   $\Phi(n) = (61-1)(53-1) = 3120$
4. Choose $e > 1$ co-prime to 3120: $e = 17$
5. Compute d such that $de \equiv 1 (\mathrm{mod}\ \phi(n))$
   e.g., by computing the modular multiplicative inverse of e modulo $\phi(n)$: $d = 2753$ since $17 \cdot 2753 = 46801$ and mod

(46801, 3120) = 1 this is the correct answer. Thus the public key is (n = 3233, e = 17). For a paddedmessage m the encryption function is:
c = me mod n = m17 mod 3233. The private key is (n = 3233, d = 2753). The decryptionfunction is: m = cd mod n = c2753 mod 3233 For example, to encrypt m = 123, we calculate c = 12317 mod 3233 = 855 To decrypt c = 855, we calculate m = 8552753 mod 3233 = 123

Symmetric Key

Symmetric algorithms, sometimes called conventionalalgorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and thedecryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that the sender and receiver agree on akey before they can communicate securely The security of a symmetric algorithm rests in the key,divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret. Usually Public Key or any other key management algorithms are used to exchange the keys before the communication takes place.Encryption and decryption with a symmetric algorithm
are denoted by:
Ek (M) = C
DK(C) = M

CONCLUSION

This paper presented the design and the simulation of a key distribution scheme over mobile ad hoc network, based on the certificateless cryptography and threshold secret sharing scheme. In this work, we have successfully issued public/ secret keys for users without providing certificates. Our scheme also ensures that system can work on self-organized networks after the initiation. From the simulation we found out that our scheme works extremely well in a small size of MANET. It reduces both packet drop rate and route discovery time for around 30 per cent, compared withpure AODV networks.

REFERENCES

1. R.L.Rivest A.Shamir L.Adleman. Certificateless public key cryptography. pages 120–126. *Communications of the ACM.* 21, 1978.
2. J.Van Der Merwe D. Dawoud S. McDonald. A survey on peer-to-peer key management for mobile ad hoc network. pages Article 1 (April pages. *ACM Comput. Surv*. **39**: 1 (2007).
3. S.S.Al-Riyami K.G.Paterson. Certificateless public key cryptography. page 452C473. C.S. Laih (ed.) Advances in Cryptology C Asiacrypt 2003, Lecture Notes in Computer Science (2003).
4. D.Boneh M.Franklin. Identity-based encryption from weil pairing. pages 586–615. *SIAM J. Computing* 32(3) (2001).
5. H.Luo P.Zerfos J.Kong S.Lu L.Zhang. Selfsecuring ad hoc wireless networks. Proceedings of the Seventh International Symposium on Computers and Communications (ISCC02).
6. S.Yi R.Kravers. Practical PKI for ad hoc wireless networks. Tech. rep. UIUCDCS-R-2002- 2273, UILU-ENG-2002-1717. Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL.
7. W.G.Wang T.Hara M.Tsukamoto S.Nishio. Aodv compatible routing with extensive use of cache information in ad-hoc networks. Proceedings of the 2002 ACM symposium on Applied computing (2002).
8. L.Zhou Z.J.Hass. Securing ad hoc networks. Pages 13,6,24–30. IEEE Netw, (1999).
9. C.Bettstetter. Mobility modeling in wireless networks:categorization, smooth movement, and border effects. ACM SIGMOBILE Mobile Computing and Communications Review, **5**(3): (2001).
10. E.Belding-Royer S.Das C.Perkins. Ad hoc ondemand distance vector (aodv) routing. RTF 3561 (2003).
11. Whitfield Diffie and Martin Hellman. New directionsin cryptography. *IEEE IT*, 22:644–654, 1976.
12. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, November 1979.
13. Adi Shamir. Identity-based cryptosystems and signature schemes. *Advances in Cryptology* -Crypto ’84, *Lecture Notes in Computer Science.* **196**: 47–53 (1985).
I4. P. Guan, Cellular Automaton Public-Key Cryptosys- Cellular Automata, IEEE Tmns. on Computers, v. 49, tern, Complex Systems I, 1987, pp. **51-56**(10): 1140-l 151 (2000).
15. H. Gutowitz, Cryptography with Dynamical Systems,
16. S. Wolfram, Cryptography with Cellular Automata, in E. Goles and N. Boccara (Eds.) Cellular Au- in Advances in Cryintology: Cry,nto ‘85 Proceedings,tomatu and Cooperative Phenomena, Kluwer Aca- LNCS 218, Springer, 1986, 429-432 (1993).
17. T. Habutsu, Y. Nishio, 1. Sasae, and S. Mori, A Secret Key Cryptosystem by Iterating a

Chaotic Map, *Proc.ofEurocrypt.*, **91**: 127-140 (1991).

18. P. D. Hortensius, R. D. McLeod, and H. C. Card, Parallel random number generation for VLSI systems using cellular automata, *IEEE Truns. on Computers.* **38**: 1466-1473 (1989).
19. J. Kari, Cryptosystems based on reversible cellular automata, personal communication (1992).