Secured Approach to Routing in Mobile Ad Hoc Networks

Rajdeep Singh
M. Tech(CTA),
SOIT, RGPV, Bhopal

Vaishali Gupta
M. Tech(IT),
NIIST, RGPV, Bhopal

ABSTRACT

The main objective is to put an effort to improve security in routing protocols, especially Clustered routing Protocol using concepts of Threshold Cryptography of distributed key management and certification. Today, networks security, whatever they are wireless or not, is an important component in the network management. The works done and studied so far are limited either up to one hop networks or for application layer services only. This work thus has been proposed to implement threshold cryptography over Clustered Based Routing Protocol.

This work thus has been proposed to implement threshold cryptography over Clustered Based Routing Protocol and to study its behavior of packet flow on the basis of average packet delay in which key size is compared versus number of shareholders.

Keywords: Mobile Ad Hoc Networks, Key Management, Threshold Cryptography, Clustered Routing

1. INTRODUCTION

Ad hoc networks are vulnerable to various kinds of attacks. Wireless communication links can be eavesdropped on without noticeable effort and communication protocols on all layers are vulnerable to specific attacks. In contrast to wired networks, known attacks like masquerading, man-in-the-middle, and replaying of messages can easily be carried out. Since providing security support for ad hoc wireless networks is challenging for a number of reasons :***(a)*** Wireless networks are susceptible to security attacks ranging from passive eavesdropping to active interfering and denial-of-service attacks. ***(b)*** Ad hoc networks provide no infrastructure support. ***(c)*** Mobile nodes may constantly leave or join the network. ***(d)*** Mobility-induced wireless link breakage/reconnection and wireless channel errors make timely communications over multi-hop highly unreliable. ***(e)*** A scalable solution is a must for a large scale network.

This approach considers the hierarchical routing environment consisting clusters having cluster-heads, normal nodes and gateway nodes and implements a distributed certificate authority among K cluster heads. Decentralization is achieved using threshold cryptography proposed by A. Shamir [3] and a network secret that is distributed over a number of nodes. While this basic idea has been proposed earlier [1, 2], its application on a clustered network on routing layer with Cluster Based Routing Protocol is a novelty of this work.

2. BACKGROUND & RELATED WORKS

Several works regarding distribution of key and distributed certification services has been proposed such as [1] describes a partially distributed PKI solution. It differs from the solution described above by the fact that the services provided by the CA, except the certification service, are distributed to specialized nodes in the network called servers. This solution assumes that a subset of nodes is able to take on the specialized server role and that every node has a minimum of K neighbor servers.

Another approach was taken in [12], where any node can play the role of server. In this approach a dealer (which is a mobile node) initializes k nodes with shares of a RSA-based private key, which these nodes then propagate through the network. If a node wants to sign a request by the DCA, a threshold of nodes must be in the vicinity (one routing hop). A join protocol was proposed that involves the cooperation of k existing nodes and two rounds of secure unicast exchange. This approach requires a dealing node to be entrusted with the DCA private key.

[2] Describes a mechanism of distributed secret sharing and certification services which achieves all basic necessities of network security and is shown over NTDR one hop networks. The idea is to distribute a CA's functionality amongst ad hoc network nodes. A Distributed Certificate Authority (DCA) is realized through the distribution of the CA's private key to a number of special shareholding DCA nodes. When CA-related operations are required, such as issuing or signing a certificate, checking public keys, or revoking certificates, a threshold of available shareholding DCA nodes should participate in the operation.

These all work mentioned above and many others like [2], [12], [14] [24] employed only either on one hop networks or on application layer services for the sake of simplicity. Here the effects of employing threshold cryptography over Clustered routing in ad hoc networks has been evaluated using Cluster Based Routing Protocol[15] in terms of Average packet delay versus different number of share holders.

3. THRESHOLD CRYPTOGRAPHY

In classic cryptography, a private key is secretly held by a user and must never be revealed, if not, security system wouldn't be reliable. Instead, in threshold cryptography, the secret is shared between several network nodes, in such a way no single node can deduce the secret without the knowing of the whole shares. The principal benefit in using threshold cryptography is to ensure security services by employing encryption without keeping the secret at only one holder, which could easily compromise.

The idea of Shamir’s (k, n) threshold system is to share a secret key between n parties [3].

Each group of any k participants (share holders), can cooperate to reconstruct the shares and recover the secret. On the other hand, no group of k-1 participants can get any information about the secret.

The Shamir’s (k, n) threshold theory is the following:

If we consider s the secret, such as s ϵ ?p, and p prime, we have to select a random polynomial f , such as:

$f(x) = f_0 + f_1x^2 + \ldots + f_{k-1}x^{k-1}$, under the condition that f (0) = s.

Where $f_1, \ldots f_{k-1} \leftarrow$ randomly

$f_0 \leftarrow s$

For i Є [1, n], the shares s_i are distributed as: $s_i = (i, f(i))$

The Shamir’s (k, n) threshold theorem stipulates that the secret s can be reconstructed from every subset of k shares. This is proven by the Lagrange formula. In fact, given k points (x_i, y_i), i = 1, . . . , k, .

$$f(x) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} \pmod p$$

And thus

$$S = f(0) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{-x_j}{x_i - x_j} \pmod p$$

The Shamir’s (*k, n*) threshold scheme announces a second theorem stipulating that any subset of up to *k*-1 shares does not leak any information on the secret. Indeed, when considering *k*-1 shares (x_i , y_i), every candidate secret *s′*Є?*p* corresponds to an unique polynomial of degree *k*-1 for which *f* (0) = *s′*. From the construction of polynomials, for all *s* Є ?*p*, probabilities Pr[*s* = *s′*] are equal. The theorem is then proven.

4. CLUSTERED ROUTING

As a result of advances in wireless technology and widespread application of wireless mobile ad hoc networks, the scale of network topology is increasing at unbelievable pace. Wireless mesh networks own large dense nodes and desires the characteristics such as self configuration, robustness, easy maintenance, low cost and most importantly Scalability [9]. Here comes the role of Hierarchical routing or what we commonly known as Clustered routing structures. Clustered Routing Structures have many prominent advantages, such as [9]:

1. During the routing, path-building phase, clustering mechanism dramatically reduces flooding overhead by decreasing the retransmission of broadcast packets.
2. During the data transmitting phase, messages that flow through the network van be further reduced by aggregating data within clusters.
3. During Routing maintenance phase, clustering mechanism made it easy to manage and handle the network changes caused by node mobility and local changes need not be seen by entire network.

Clustering approach is used to minimize on-demand route discovery traffic. The idea behind CBRP is to divide nodes of an ad hoc network into a number of overlapping or disjoint clusters. One node is elected as cluster head for each cluster. The cluster head maintains membership information for its cluster. Inter cluster routes are discovered dynamically using the membership information.

The difference is that the cluster structure generally means that the number of nodes disturbed is much less. Flat routing protocols, i.e. only one level of hierarchy, might suffer from excessive overhead when scaled up. [13]

5. PROPOSED WORK`

The work we presented here for key management in ad hoc networks and implemented it at routing layer in ad hoc networks, assume the existence of a clustering protocol which can split the network into groups that are stable enough. It uses a (K,N) threshold scheme to distribute an RSA certificate signing key to the set of cluster heads. It also uses proactive and verifiable secret sharing (which is out of the scope of this work) to protect the secret respectively from denial of service attacks and node compromise.

This architecture consists of 3 types of nodes

- ✓ Set of Cluster heads- which will provide distributed CA services
- ✓ Simple nodes.
- ✓ Administrator.

`5.1 Cluster Generation Step: We are not going to propose a new clustering protocol but to select an existing one (WCA, H-ID, Min-ID..[9].) which would be suitable for our case study concerning key management. Clustering parameters that we must take into consideration are:

1. *Clusters stability*: We prefer having clusters where the corresponding cluster heads have a minimum mobility degree.
2. *Cluster heads energy*: we had better to elect cluster heads having the highest power because they will be responsible for some tasks.

5.2 Initialization: At Initialization, we assume some mechanism proposed earlier in [2], [12], [14] [24] to distribute shares among cluster heads in our network at initial step and after that such responsibility is handed over to set of cluster heads sharing secret. Thus every CH, C_i will then possess a secret key S_i of the CA secret key which helps in securing network and handling of secret in an efficient manner. Cluster head will be then considered as a distributed CA for further scaling of network.

Following section consists of firstly an algorithm for secret sharing, i.e. it shows how a secret will be distributed over a number of shares when administrator is not present in system.

5.3Algorithm KeySharing

1. New CH contacts to administrator.
2. If latter is present, CH sends a request for initialization including its id and public key, else
3. goto (5).
4. Administrator computes a partial key to CH in following way:
   - Select a large prime number p.

- Consider a polynomial function f(x) of degree k-1 such that
  $f(x)= [S+a_1x+a_2x^2+ \dots + a_{k-1}x^{k-1}] \bmod p$,

  where k is number of nodes among which secret has been shared.
- Now, compute the partial key $S_i = f(id)$, where id is identity provided by the CH.

5. CH sends request any cluster head (shareholders) CHL, which on certifying issue him, his partial share in the following way:

- $S_{CH,I} = S_L \times Fid_L(id)$, where

$$Fid_L(id) = \prod_{L=1, j\neq L}^{k} \left\{\frac{id - id_j}{id_L - id_j}\right\}$$

- By combining, k such shares i.e. $S_{CH,I}$, we get, S_i as follows:

$$S_i = \sum_{L=1}^{k} S_{CH,I} = \sum_{L=1}^{k} S_L \times Fid_L(id)$$

$$= f(id)$$

6. End if
7. End.

6. SIMULATION & RESULTS

To evaluate the effectiveness of our approach, CBRP has been implemented in a network simulator NS2 and threshold cryptography is implemented over it and behavior is studied in terms of average packet delay. The parameters and scenarios used in this simulation are illustrated in this section in which we have simulated the approach on over environment with 50 nodes spread over two area scenarios of 670×670 metres^2 and 1500×300 metres^2 with a total simulation time of 300 seconds for both cases. In simulated environment used, the traffic type used is CBR with a packet size of 512 bytes. For simulating data transfer maximum numbers of packets shown to be transferred are 10,000 where packet send rate is 0.25 seconds/packet with maximum connection scenario of 10 node and 20 nodes. Now details regarding pause time and movement speed of nodes (which is 20 m/sec in all cases) in different scenarios assumes has been tabulated below:

Table-1: Scen_1

Simulation area of 670×670 metres^2			
Pause time	30 sec	60 sec	120 sec
Node Movement Speed	20 m/s	20 m/s	20 m/s

Table-2: Scen_2

Simulation area of 1500×300 metres^2			
Pause time	30 sec	60 sec	120 sec
Node Movement Speed	20 m/s	20 m/s	20 m/s

Now, we will illustrate the results which expound the effectiveness of work in terms of average packet delay in different scenarios mentioned above and compared with and without employing encryption. In case of with encryption three different cases of different key sizes has been considered i.e. of 128 bits, 256 bits and 512 bits key size. In implementation, number of cluster heads is considered is 10 in all cases for the sake of simplification, effectiveness is been evaluated for different number of shareholders (i.e. 3, 5, 7) among total number of cluster heads.

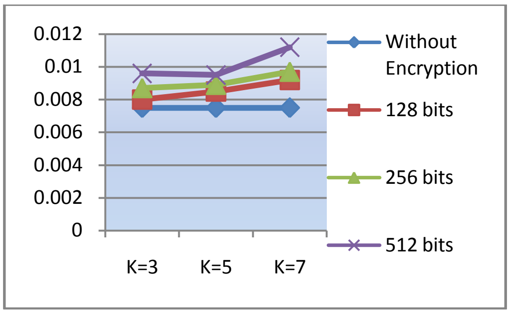

Figure1: : Average packet delay in terms of sec for case 1 of first scen i.e. for 30sec pause time for 670×670 m^2

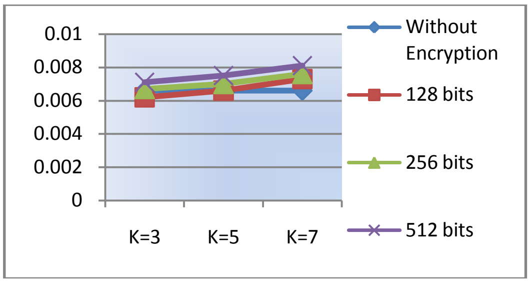

Figure2: Average packet delay in terms of sec for case 2 of first scen i.e. for 60sec pause time for 670×670 m^2

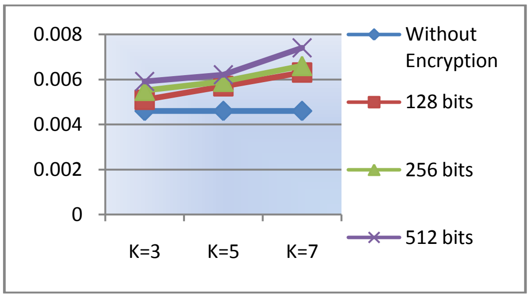

Figure3: Average packet delay in terms of sec for case 3 of first scen i.e. for 120 sec pause time for 670×670 m^2

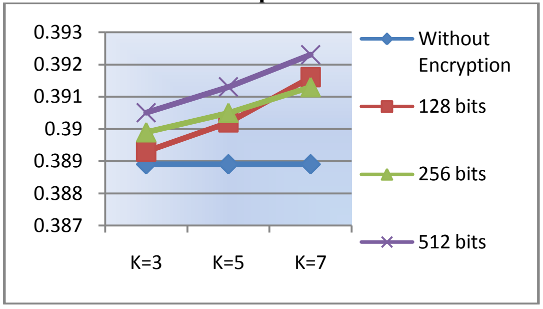

Figure4: Average packet delay in terms of sec for case 1 of second scen i.e. for 30 sec pause time for 1500×300 m^2 30sec pause time for 1500×300 m^2

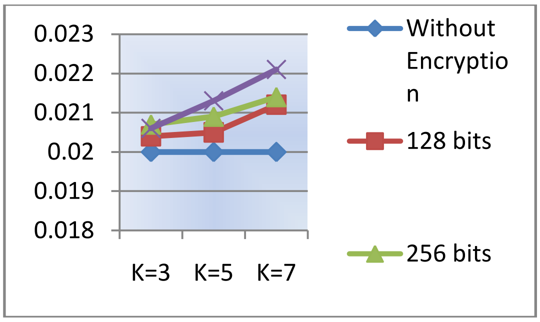

Figure5: Average packet delay in terms of sec for case 2 of second scen i.e. for 60sec pause time for 1500×300 m^2

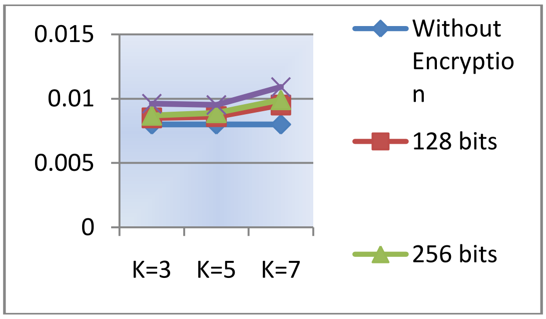

Figure 6: Average packet delay in terms of sec for case 3 of second scen i.e. for120sec pause time for 1500×300 m^2

Figure 1, 2, 3 are expounding the results of average packet delay with 50 nodes spread over scen-1 i.e. 670×670 m^2 with node movement speed of 20m/sec and respective pause time of 30s, 60s, and 120s.

Whereas, Figure 4, 5, 6 are expounding results of average packet delay with 50 nodes spread over scen-2 i.e. 1500×300 m^2 with node movement speed of 20m/sec and respective pause time of 30s, 60s, and 120s.

Above mentioned results have been plotted, which illustrates pattern of average packet delay(in seconds) versus different values of share holders(K), and it can be clearly posed from above shown results that on increasing number of shareholders, average packet delay also increases respectively. It can also be concluded that as simulation area of our simulation is increased, average packet delay drastically get increased with respective key size. It is also important to depict here that when encryption is not deployed in network, it is, but obvious that there is no role of share holders or any secret distribution therefore average packet delay is shown constant. And, lastly it is seen that comparative increase in average packet delay is more in case when we transit from number of shareholders from 5 to 7, than that of former one.

A threshold secret sharing scheme exhibits several properties which are amongst basic building blocks of a secure environment.

To secure an ad hoc network, we consider the following attributes: Availability, Confidentiality, Integrity, and Non-repudiation. Here in the work proposed, as specified earlier, that asymmetric encryption is used to secure Clustered routing protocol where (k, n) threshold scheme is used to distribute an RSA certificate signing key to the set of cluster heads, which makes the job of the attacker harder than earlier because one has to attack and compromise at least n out of k nodes to recover secret which is almost impossible. Secondly, attacks such as listening to packets could be easily resolved due to encryption used and the key used for the process is managed efficiently through threshold scheme of key distribution. Along with this, traffic analysis is also an attack where packets are analyzed, and such analysis can reveal interesting information which could be used in much more severe attacks, is also got resolved by the encryption used in efficient way.

Other attributes such as integrity, non-repudiation and availability can also be achieved by using digital signatures, certification services etc. which also in turn need the use of key management.

This work also provides the solution to single point of failure problem and a standard approach to improve availability of services is replication but compromise of any single replica could lead entire system to collapse. To solve this problem, we distribute the secret/trust to a set of nodes by letting these nodes share the key management responsibility.

Ultimately, the purpose of the approach is to illustrate and expound the behavior of the network in terms of packet flow is not degraded too much and is considerable with context to secure environment achieved.

7. CONCLUSION

The present work is carried in the general context of security study in ad hoc networks. We focused on key management problem in such networks and tried to implement it and evaluate it through Threshold Cryptography concept proposed by Shamir by employing it on Cluster Based Routing Protocol. The work consists in analyzing effects of employing secret sharing mechanism over clustered routing in ad hoc networks to palliate their limitations which ensures better and secure environment, which shows that with increase in key size as well as number of share holders there is gradual increase in average packet delay too for more or less every case. Thus, in a first stage, we focus our interest on existing key management solutions for ad hoc networks proposed in the literature. And, secondly one is chosen and evaluated. Distributed architectures are more suitable to ad hoc networks which are peer to peer networks and where the client/server model is a little bit adaptable. We can say that our work permits to settle down a key management solution which is adaptable regarding ad hoc networks constraints especially the lack of infrastructure, energy limitations and mobility. It tempts to resolve key distribution problems using a locally centralized solution for the nodes of each cluster and a globally distributed solution for cluster heads. This has a great advantage concerning security services availability. Moreover, concept of proactive secret updates can also be employed to enhance the overall security of the network by periodically updating of shares among shareholders with variable number of cluster heads with course of time and can be compared with other routing schemes of ad hoc networks.

8. REFERENCES

[1] Lidong Zhou, Zygmunt J. Haas, Cornell University, Ithaca, NY, “Securing Ad Hoc Networks”, IEEE Network, 1999.

[2] Ghassan Chaddoud, Department of Scientific Services, Atomic Energy Commission of Syria, Keith Martin, Information Security Group, Royal Holloway, University of London, “Distributed Certificate Authority in Cluster-based Ad hoc networks”, ICMU 2006.

[3] Adi Shamir, Massachusetts Instt of Technology, “How to Share a secret”.

[4] Subhankar Das, San Jose State University, “MANET: Applications, Issues and Challenges for the Future”, Int’l J. of Business Data Communications and Networking, 1(2), 66-92, April-June 2005.

[5] Charles E. Perkins, “Ad Hoc Networking” Pearson Education, 2001.

[6] Krishna Gorantala, “Routing Protocols in Mobile Ad-hoc Networks”, UMEA University, Sweden, 2006.

[7] Elizabeth M. Royer, University of California, Santa Barbara, Chai-Keong Toh, Georgia Institute of Technology, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communications, April 1999.

[8] Ching-Chuan Chiang, Hsiao-Kuang Wu, Winston Liu, Mario Gerla Computer Science Department University of California, Los Angeles, “Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel” Proc. IEEE SlCON '97, Apr. 1997, pp. 197-211.

[9] Jian Wan, Daomin Yuan, Xianghua Xu, Grid and Services Computing Lab, Hangzhou Dianzi University Hangzhou, China, “A Review of Cluster Formation Mechanism for Clustering Routing Protocols”,11th IEEE International Conference on Communication Technology roceedings, 2008.

[10] Yang Qin, School of EEE Nanyang Technological University Singapore, Kong Ling Pang Research and Development Division Olympus Technologies Singapore Pte Ltd Singapore, “A Fault-tolerance Cluster Head Based Routing Protocol for Ad Hoc Networks”, IEEE, 2008.

[11] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, and Lixia Zhang, “Providing Robust and Ubiquitous Security Support for Wireless Mobile Networks”, *Ninth International Conference on Network Protocols (ICNP’01)*, pages 251–260, 2001.

[12] Tony Larsson, Nicklas Hedman, Lulea University of Technology, Stockholm “Routing protocols in Wireless Ad-hoc Networks- A Simulation Study”, 1998.

[13] Haiyun Luo, Songwu Lu, Computer Science Department University of California, Los Angeles Los Angeles, CA 90095-1596, “Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks”October 2000.

[14] Mingliang Jiang, Jinyang Li, Y.C. Tay, draft-ietf-manet-cbrp-spec-01, 14 August 1999.

[15] R.L. Rivest, A. Shamir, and L. Adleman, Massachusetts Institute of Technology, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”.

[16] M. Gerla and J. T. C. Tsai, “Multicluster, Mobile Multimedia Radio Networks”, wireless networks vol.I 1995, pp. 255-265.

[17] Kaixin Xu, Xiaoyan Hong, M. Gerla, “An Ad hoc Network with Mobile Backbones”, ICC 2002. IEEE International Conference, Volume 5, 2002, pp. 3138-3143.

[18] C.R. Lin, and M. Gerla, “Adaptive Clustering for Mobile Wireless Networks”, IEEE Journal on selected arrears in communications, Vol. 15, No.7, Seq. 1997, pp. 1265-1275.

[19] Alia Fourati, Khaldoun Al Agha, “A shared secret-based algorithm for securing the OLSR routing protocol”, 2005

[20] Arun Khetrapal, Deptt. Of Computer Engineering, Delhi College of engineering, Delhi University, “Routing Techniques for Mobile Ad Hoc Networks Classification and Qualitative/ Quantitative Analysis”.