An Efficient Routing Approach to provide Security in Wireless Networks

[1]Dr.Vasumathi [2]N.Sainath

[1]Associate Professor , Department of CSE Additional Controller of Examinations-4,
JNTUH ,Kukatpally , Hyderabad.

[2]Research Scholar , Department of CSE, JNTUH ,Kukatpally , Hyderabad.
, Andhrapradesh.
E-Mail : natukulasainath@gmail.com Mob:9440590561

Abstract — Wireless adhoc network is autonomous, infrastructure less and may be mobile depending on its type of application. Secure transmission of information in wireless adhoc environment is an important concern. In this paper we propose to use shared cryptography to secure message communication in adhoc network. In this approach we divide any information into multiple shares and transmit the different shares via multiple disjoint paths between any pair of communicating nodes and if possible at different point of time. At the receiving end the original information is reconstructed by combining the shares received via different paths at different point of time. We have also proposed to keep redundancy in the number of shares to withstand loss of some shares due to loss in transmission or security attacks.

Compared to other available schemes, it has minimal computational complexity. That makes it more effective in energy saving distributed environment where battery driven low end processors are used and security is also a major challenge.

Keywords – **Adhoc Network, Security threats, Threshold Cryptography, Information sharing;**

1. INTRODUCTION

The Advancement in the decade is lot in the stream of Mobile Adhoc Networks The increase of cheaper, smaller and more powerful mobile devices have made wireless adhoc networks to become one of the fastest growing areas of research. This new type of self-deploying network may combine wireless communication with high degree node mobility. Unlike conventional wired networks they have no fixed infrastructure. This flexibility makes them attractive for many applications for a situation where either supporting structure is unavailable or deployment is unfeasible such as military networks and disaster recovery operations . The adhoc self-organisation also makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time consuming high-cost task.

Security is an indispensable need for both wired and wireless network communications. Unlike wired networks, wireless networks pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc.

There are a wide variety of attacks that target the weakness of this kind of network. In this type of network, security is not a single layer issue but a multilayered one. We have focused on network layer where the possible attacks are most vulnerable.

Some of the attacks which we tried to address are Black hole, Gray hole, Worm hole, Jellyfish attack, Spoofing and Sybil attack.

Due to the above mentioned network layer threats, the transmission of extremely sensitive information via one single path is not advisable as the information can easily be lost or hacked if the individual path is not fully trusted. To avoid this threat sender may want to send multiple copies through multiple disjoint paths. But this increases the risk of information leakage.

Shared cryptography tries to address this concern. It transmits different shares of the information via multiple disjoint paths at different interval of times. It forces the shares received individually to co-operate for reconstructing the information at the receiving end. This not only reduces the risk of information leakage but also reduces the chance of several possible network level attacks in wireless environment.

In threshold cryptography , secret sharing deals with such difficulty. This approach shares a highly sensitive secret among a group of n users so that only when a sufficient number k (k<= n) of them come together, the secret can be reconstructed. Well known secret sharing schemes (SSS) in the literature include Shamir [9] based on polynomial interpolation, Blakley [10] based on hyper plane geometry and Asmuth-Bloom [11] based on Chinese Remainder theorem.

All these approaches lead to high computational complexity during both sharing and reconstructing the information. Our scheme employs simple graphical masking method, done by simple AND-ing for share generation and reconstruction can be done by simple OR-ing the qualified set of shares.

This makes the computational complexity very minimal compared to the earlier proposed schemes. This makes it effective for addressing energy saving distributed environment where battery driven low end processors are used and security is also a major challenge.

This paper is structured as follows. In section 2 we have described different network layer threats in wireless ad-hoc network. In section 3 we have described our secret sharing scheme. We have described how our scheme can countermeasure the possible network layer attacks in section 4. Finally section 5 concludes the paper.

2. OVERVIEW OF NETWORK LAYER THREATS

Before going into the details of our proposed scheme, first let us characterize the network layer threats in brief.

Black hole: In a black hole attack a malicious node advertises itself as having a valid route to the destination node even though the route is spurious. With this intension the attacker consumes or intercepts the packet without forwarding it. The attacker can completely suppress or modify the packet and generate fake information, which may cause network traffic diversion or packet drop.

We have proposed to send these shares at different point of time, if possible. At the receiving end the original information is reconstructed by combining the received shares. We have also proposed to keep redundancy in the number of shares to withstand loss of some shares due to loss in transmission or security attacks.

The earlier schemes are based on polynomial interpolation, hyper plane geometry involving matrix inversion or Chinese Remainder theorem. Those lead to high computational complexity during both sharing and reconstructing.

Worm hole: A worm hole attack is where two or more malicious nodes may collaborate to encapsulate and exchange messages between them along existing data routes. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. A worm hole shows a valid route to the destination but it always tunnels the packet to its malicious partner node. This attack is also known as tunneling attack.

Jellyfish attack: In jellyfish attack the malicious node first intrudes into the forwarding group in the network and then it unreasonably delays data packets for some amount of time before forwarding them. This result in significantly high end-to-end delay and delay jitter, and thus degrades the performance of real-time applications.

Spoofing: This occurs when a malicious node pretends other node’s identity at times. This in turn misguides a non malicious node in order to alter the vision of the network topology that it can gather.

Sybil attack: In this attack, attacker pretends to have manifold identities/nodes. A malicious node can act as if it were a multiple number of nodes either by impersonating other nodes or simply by claiming false identities. This allows him to forge the result of a voting used for threshold security methods for more information.

Gray hole: Gray hole is a node in the established routing topology that selectively drops packet with certain probability causing network distraction. Gray hole may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole may behave maliciously for some time period by dropping all packets but may switch to normal behaviour later. A gray hole may also exhibit a behaviour which is a combination of the above two.

3. OUR SCHEME

In our scheme we have proposed to divide any information into multiple shares. These different shares are to be transmitted via multiple disjoint paths between the pair of nodes.

The success of our scheme depends upon the mask generation. A step wise algorithm is suggested for such mask design for any **(n, k)** scheme where **n** number of masks are designed to generate **n** different shares and any **k** shares on ORing reconstruct the original secret.

Before we describe the scheme let us enumerate some assumptions which are quiet trivial.

- Each node is identified with a unique nonzero identification number.
- All nodes in the network are aware of the total number of nodes at the beginning.
- Network starts with all non-malicious nodes at the beginning.
- Network is connected i.e. there is a route between any pair of nodes.
- Communication is bidirectional between any pair of nodes.
- Multiple numbers of routes are available between two pair of nodes.
- Network starts with fixed value of **n** and **k**. i.e., all the non malicious nodes at the beginning are aware about the number of shares and the threshold value.

3.1 Secret Sharing Algorithm Concept

For better understanding let us consider any secret as a binary bit file (i.e. bit is the smallest unit to work upon, in actual implementation one can consider a byte or group of bytes or group of pixels as the working unit) . The secret could be an image, an audio or text etc. We shall decompose the bit file of any size onto **n** shares in such a way that the original bit file can be reconstructed only ORing any **k** number of shares where **k n 2** but in practice we should consider **2 k<n 3**.

Our basic idea is based on the fact that every share should have some bits missing and those missing bits will be replenished by exactly **(k-1)** other shares but not less than that. So every individual bit will be missed from exactly **(k-1)** shares and must be present in all remaining **(n-k+1)** shares, thus the bit under consideration is available in any set of **k** shares but not guaranteed in less than **k** shares. Now for a group of bits, for a particular bit position, **(k-1)** number of shares should have the bit missed and **(n-k+1)** number of shares should have the bit present and similarly for different positions there should be different combinations of **(k-1)** shares having the bits missed and **(n-k+1)** number of shares having the bits present. Clearly for every bit position there should be $^{n}C_{k-1}$ such combinations and in our scheme thus forms the mask of size $^{n}C_{k-1}$, which will be repeatedly AND over the secret in any regular order. Different mask will produce different shares (The style of placing the mask over the secret could be anything but it will be same for every share. It may also be noted that the knowledge of positioning the masks over the secret is not at all required for reconstruction of the secret) from the secret. Thus 0 on the mask will eliminate the bit from the secret and 1 in the mask will retain the bit forming one share. Different masks having different 1 and 0 distributions will thus generate different shares.

Next just ORing any **k** number of shares we get the secret back but individual share having random nos. of 1's & 0's reflect no idea about the secret. As an example a possible set of masks for 5 shares with threshold of 3 shares is shown below:

Mask 1:	**0 0 0 0 1 1 1 1 1 1**
Mask 2:	**0 1 1 1 0 0 0 1 1 1**
Mask 3:	**1 0 1 1 0 1 1 0 0 1**
Mask 4:	**1 1 0 1 1 0 1 0 1 0**
Mask 5:	**1 1 1 0 1 1 0 1 0 0**

One can easily check that ORing any three or more shares we get all 1's but with less than three shares some positions still have 0's i.e. remain missing.

3.2 Mask Designing Technique

The algorithm for designing the masks for **n** shares with threshold **k** is as follows.

Step 1: List all row vectors of size **n** having the combination of **(k-1)** nos. of **0's** and **(n-k+1)** nos. of **1's** and arrange them in the form of a matrix. Obvious dimension of the matrix will be $^{n}C_{k-1} \times$ **n.**

Step 2: Transpose the matrix generated in Step-1. Obvious dimension of the transposed matrix will be **n** × $^{\mathbf{n}}\mathbf{C}_{\mathbf{k-1}}$. Each row of this matrix will be the individual mask for **n** different shares. The size of each mask is $^{\mathbf{n}}\mathbf{C}_{\mathbf{k-1}}$ bits, i.e. the size of the mask varies with the value of **n** and **k**. (It may be noted that the masking patterns are not unique. Different arrangements of the row vectors in Step-1 leads to different sets of masks but for a particular set, the masks are unique and they satisfy the requirements)

Let us consider the previous example where **n**=5 and **k**=3.

Step 1: List of row vectors of size 5 bits with 2 numbers of 0's and 3 nos. of 1's.

$$\begin{matrix} \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{matrix}$$

Dimension of the matrix is $^{\mathbf{5}}\mathbf{C}_{2}$ **× 5** i.e. **10 × 5**

Step 2: Take the transpose of the above matrix and we get the desired masks for five shares as listed above in the form of matrix of dimension **5** × $^{\mathbf{5}}\mathbf{C}_{2}$ i.e. 5 x 10. There are five masks each of size 10 bits.

3.3 Total Information Management

The sending node generates n unique shares from the original information by masking the original one repeatedly with each individual mask (technique of generating n unique masks is already discussed).

Next the sending node starts sending all n shares to the destination using as many possible disjoint paths asynchronously i.e. .no two shares are sent simultaneously.

Now at the destination any k nos. of received shares (assumed that the destination node has received at least k shares as **n** nos. of shares are been transmitted and **n** is larger than **k**) are logically ORed to reconstruct the original information.

The number of shares transmitted is always larger than **k**, the minimum number of shares needed to reconstruct the original. This redundancy in number of shares allows the loss in transmission or due to the presence of security attacks, which makes the system robust towards different network layer threats

4. Strength of Our Algorithm

We now explain how our scheme can reinforce any wireless ad-hoc network against various security threats at the network level. Our basic idea of sharing, transmitting the shares asynchronously via multiple disjoint paths and redundancy in the number of shares well addresses more or less all common possible network layer attacks.

Black hole: In our scheme the information is shared through multiple routes, and the number of shares is more than the number that is needed to reconstruct the message. So even if there is a black hole in a particular route, the destination can easily construct the information from other available shares coming through other routes.

Gray hole: This is also addressed similarly as in the black hole. The receiving node is also capable of reconstructing the actual information without the lost share even if there is a Gray hole.

Worm hole: Tunneling one share to its counterpart of any malicious node will not affect the share reaching to the receiving node. On the other hand, as the information is shared the malicious partner node cannot get the total information by having a single share.

Jellyfish attack: Information is shared. Therefore just by delaying one route (i.e. one share) will not harm the reconstruction phase of the information at the receiving end.

Spoofing: This attack can be responsible for the missing of one share. But it is again easily possible for the receiving node to reconstruct the information from the other shares.

Sybil attack: Sybil attacker can get a threshold number of shares to construct the original information. But a time delay in the sending phase of the shares will not allow the Sybil attacker to collect the minimum number of reconstruct able shares.

5. CONCLUSION

In this paper we have proposed a novel security scheme for wireless ad -hoc network based on shared information. We have proposed to keep redundancy in the number of shares to withstand loss of some shares due to transmission loss as well as due the presence of network layer security threats.The scope of our future work is not only to withstand the loss but also to identify the malicious route and may be the intruder node itself.

REFERENCES

[1] Internet Engineering Task Force (IETF) Mobile Ad Hoc Networks (MANET) Working Group Charter, www.ietf.org/html.charters/manet-charter.html J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon,2005, pp 68–73.

[2] T.S. Rappaport, Wireless Communications: Principles and Practice, Prentice Hall, Upper Saddle River, NJ, Oct. 2005

[3] Hassan A. Karimi, Prashant Krishnamurthy "Real-time routing in mobile networks using GPS and GIS techniques", Proceedings of the 34th IEEE Hawaii International Conference on System Sciences – 2009

[4] Luiz A. DaSilva, Jeff H. Reed, William Newhall, Tutorial on "Ad hoc networks and automotive applications", Mobile and Portable Radio Group, Virginia Polytechnic Institute and State University, 2010

[5] HongMei Deng, Wei Li, Dharma P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, October 2011, pp70-75

[6] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A survey on attacks and countermeasures in mobile ad hoc networks", Wireless/Mobile Network Security, chapter 12, pp 1-38, Springer, 2006

[7] Y. Desmedt "Some recent research aspects of threshold cryptography" Proc of ISW'97 1st International Information Security Workshop vol.1196 of LNCS pp 158-173 Springer-Verlag 2007.

[8] Y. Desmedt and Y. Frankel "Threshold cryptosystems" Proc of CRYPTO'89 volume 435 of LNCS, pp 307-315 Springer Verlag 2011

[9] A. Shamir: "How to share a secret?" Comm ACM, 22(11): pp612-613, 1979.

[10] G. Blakley : "Safeguarding cryptographic keys " Proc. of AFIPS National Computer Conference, 1979

[11] C. Asmuth and J. Bloom :"A modular approach to key safeguarding" IEEE transaction on Information Theory, 29(2):pp 208-210, 1983.

Author's Information :

[1]Dr.D.Vasumathi PhD from JNTU Hyderabad .Currently working as Additional Controller of Examinations-4 in JNTU Hyderabad .She is also Associate Professor for the department of CSE and has a vast teaching experience . Her areas of interest are Dataming , Network Security , Adhoc Networks , Software Engineering , Cloud computing.

[2]**N.Sainath** B.Tech CSE from JayaPrakash Narayana College of Engineering M.Tech SE from Srinidhi Institute of Technology. Currently he is Research Scholar at JNTU Hyderabad . His areas of interest include Data mining, Network Security, Software Engineering, Sensor Networks , Cloud Computing. He is Enrolled for the Professional memberships of IEEE, CSI, MISTE, IAENG , CSTA. He has Published 12 papers in International Journals and has 4 International conference Proceedings and attended 12 workshops and 10 National conferences.