Enhanced Novel Security Scheme for Wireless Adhoc Networks: ENSS

Prasad Patil
Vidyalankar Institute of Technology
Wadala(E), Mumbai

Rinku Shah
Vidyalankar Institute of Technology
Wadala(E),Mumbai

Kajal Jewani
Vidyalankar Institute of Technology
Wadala(E), Mumbai

ABSTRACT

In recent years, a lot of research is focused on wireless adhoc network, which is focused on field of performance, security, and energy. This paper addressed the difficulties and challenges facing the adhoc networks in security. 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. In this paper Novel Security Scheme for Wireless Adhoc Networks (NSS) is studied and some serious drawbacks of NSS have been realized. To overcome these drawbacks, Enhanced Novel Security Scheme (ENSS) is proposed. Classical approaches of secret sharing have high computational complexity. While proposed approach (ENSS) provides high security with moderate computational complexity results in less power consumption.

General Terms

Wireless Adhoc Networks, Security, and Shared cryptography.

Keywords

Novel security scheme, Enhanced Novel security scheme

1. INTRODUCTION

Ad hoc networking enables wireless devices to network with one another, as needed, even when access to the Internet is unavailable. It enables a wide range of powerful applications, from instant conferencing between notebook PC users to emergency and military services that must perform in the harshest conditions [1]. Wireless communication should be possible without routers, base stations or Internet Service Providers. An ad-hoc network might consist of several home-computing devices, plus a notebook computer that must exist on home and office networks without extra administrative work. Key applications of ad-hoc networking are conferencing, home networking, emergency services, Personal Area Networks, Bluetooth, and more. The key challenges of ad hoc networking are resource management, scalability, and especially security.

Although ad hoc networks have several advantages over the traditional wired networks, on the other side's they have a unique set of challenges [4].

Firstly, adhoc networks face challenges in secure communication. For example the resource constraints on nodes (viz. power consumption) in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion.

Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network.

Thirdly, static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like DoS (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information.

We have studied the Novel Security Scheme [2] for wireless adhoc networks (NSS) that is based on shared cryptography .We found some serious drawback of the scheme. These drawbacks harm confidentiality, integrity of the data in communication using NSS. To overcome these drawbacks we have proposed an Enhanced Novel Security Scheme (ENSS) for wireless adhoc networks.

Section 2 consists of literature survey regarding constraints in wireless adhoc networks. Section 3 describes the NSS and its drawbacks. Section 4 proposes Enhanced method for NSS. Then Section 5 compares NSS and ENSS approach. Finally conclusion is drawn in section 6.

2. LITERATURE SURVEY – CONSTRAINTS ON SECURITY IN WIRELESS ADHOC NETWORKS

There are a wide variety of attacks [3] 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 that we tried to address are Black hole, Gray hole, Wormhole, 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. Share is a copy of a original data in which some bits are present and some bits are missing. 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 [5,6], 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 arrives together, the secret can be reconstructed. Well known secret sharing schemes (SSS) in the literature include Shamir [7] based on polynomial interpolation, Blakley [7] based on hyper plane geometry and Asmuth-Bloom [9] based on Chinese Remainder theorem.

All these approaches lead to high computational complexity during both sharing and reconstructing the information. So there is need for addressing energy saving distributed environment where battery driven low-end processors are used and security is also a major challenge.

3. NOVEL SECURITY SCHEME

In this approach [2] it has been proposed to divide any information into multiple shares. These different shares are to be transmitted via multiple disjoint paths between the pair of communicating nodes .NSS 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. Share is a copy of the original data in which some bits are present and some bits are missing. It has 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 NSS scheme employs ANDing operation for share generation. At receiver side to regenerate original message ORing operation is carried out. The energy saving distributed wireless networks having need of high security but constrained by battery driven low end processors will get attracted by the minimal computational complexity of NSS scheme.

Consider the secret to be transmitted as binary bit file. 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. Basic idea is based on the fact that every share should have some bits missing. The missing bits will be replenished by exactly (k-1) other shares. 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 this scheme thus forms the mask of size $^{n}C_{k-1}$, which will be repeatedly ANDed 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.

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

3.1 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 $n \times {}^{n}C_{k-1}$. Each row of this matrix will be the individual mask for n different shares. The size of each mask is $^{n}C_{k-1}$ bits, i.e. the size of the mask varies with the value of n and k.

3.2 Example

Let us assume that node A wants to send a secret to node B. The secret of node A is 1100101001. Assume that n=5, i.e. 5 different paths are available from node A to node B. Let the threshold value k=3, i.e. by receiving k no of shares node B can regenerate original message but not less than that.

Mask designing for n=5 and k=3.

Step 1: List of all row vectors possible combinations of 1 and 0 where there are exactly 3 no of 1's and 2 no of 0's because n=5 and k=3.

$$\begin{bmatrix} 0\,0\,1\,1\,1 \\ 0\,1\,0\,1\,1 \\ 0\,1\,1\,0\,1 \\ 0\,1\,1\,1\,0 \\ 1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1 \\ 1\,0\,1\,1\,0 \\ 1\,1\,0\,0\,1 \\ 1\,1\,0\,1\,0 \\ 1\,1\,1\,0\,0 \end{bmatrix}$$

Step 2: Taking transpose of the above matrix. So each row will be the mask for n different paths.

Mask 1: 0000111111
Mask 2: 0111000111
Mask 3: 1011011001
Mask 4: 1101101010
Mask 5: 1110110100

Now apply each mask over the secret.

Secret – 1100101001 AND mask 1- 0000111111 -------------------------------- Share 1 → 0000101001	Secret- 1100101001 AND mask 2- 0111000111 ------------------------------- Share 2 → 0100000001
Secret – 1100101001 AND mask 3- 1011011001 -------------------------------- Share 3 → 1000001001	Secret- 1100101001 AND mask 4- 1101101010 ------------------------------- Share 4 → 1100101000

Secret – 1100101001
AND mask 5- 1110110100

Share 5 → 1000100000

The node A generates these shares. Now these shares are sent via 5 different paths asynchronously.

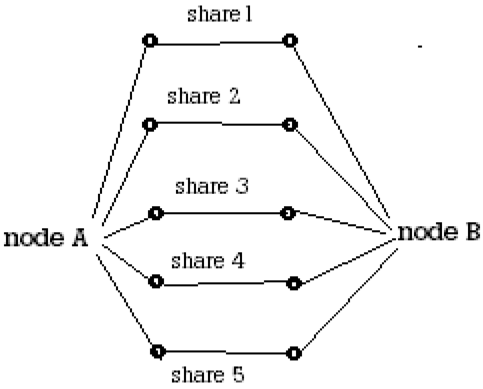

Fig 1: Multi path share sending

Now at the receiver side node B, original message is recovered by performing OR operation on received shares

	0000101001	share 1
OR	0100000001	share 2
OR	1000001001	share 3
OR	1100101000	share 4
OR	1000100000	share 5
	1100101001	Original message

Suppose, it can be happen that share 2 and share 5 lost in network. As our threshold value is k=3, receiver must generate original data.

	0000101001	share 1
OR	1000001001	share 3
OR	1100101000	share 4
	1100101001	Original message

3.3 NSS Operation

The sending node generates n unique shares from the original information by masking the original one repeatedly with each individual mask

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.

3.4 Advantages

The operations are carried out just ORing and ANDing so the low computational capability is needed.

Low computation power is needed hence energy of wireless nodes is saved.

Since secret is shared via different paths, possibility of information leakage is very low.

This scheme addresses the issue of multiple copies or parted message.

The scheme also addresses the issue of high security with low computational complexity.

3.5 Drawbacks of NSS

- In NSS all the shares are sent asynchronously. NSS approach did not mentioned about the time framework. So it is unclear that how much receiver should wait? The system is supposed to be deployed in emergency fields in which communication should be as fast as possible. It is based on assumption that shares will reach, which may not be true.
- In NSS value of the threshold is unknown to the receiver. Again it relies on network characteristics that might change in future. There is no facility of detecting malicious route.
- It can happen that a malicious node manipulates the bits of particular share and forwards it. In this case false data can be generated on the receiver side. If there exist malicious node that could tamper the share, integrity is lost.

Now suppose a node wish to send two consecutive secrets to same receiver. As data is being transmitted asynchronously, there can be delay in packet arriving. There is no mechanism to differentiate shares of two different messages.

E.g. In the example described above, suppose share 4 is passed through malicious route and malicious node manipulates bits of share 4. As result false data is generated. Assume that share 4 is manipulated as 1111101000 instead of 1100101000.

So at receiver side

	0000101001	share 1
OR	0100000001	share 2
OR	1000001001	share 3
OR	1111101000	share 4 (forged by malicious node)
OR	1000100000	share 5
	1111101001	false secret is generated at receiver

Above mentioned serious issues need to be resolved.

4. ENHANCED NOVEL SECURITY SCHEME FOR WIRELESS ADHOC NETWORKS: ENSS

ENSS proposes an enhanced scheme for more reliability of the novel scheme. ENSS proposes a mechanism to protect integrity of the data. Core concept of message sending using shared cryptography remains unchanged.

4.1 ENSS Algorithm

1) Sender counts the paths available for the transmission i.e. it decides the value of n.
2) The sender decides value of threshold (k).
3) The sender designs the mask according to values of n & k.
4) The sender applies the mask and generates the shares.
5) Each share of same message is assigned a unique number.
6) The sender sends the shares via multiple disjoint paths.
7) Each path is assigned a number.
8) Among the n paths one path is randomly chosen.
9) The information about threshold value, paths assigned and message hash value is send via this path encrypted using one of following way
→Public key encryption
→Symmetric key encryption (in presence of human)
.

Only hash value, threshold value and paths assigned sent secured via random path. The whole idea of the shared cryptography and mask generation remains unchanged in ENSS.

The following modifications are suggested by ENSS:

- Each path is assigned a number that will be helpful in deciding malicious route.
- The unique number assigned for each share of same message helps receiver to differentiate different message from same sender.
- Since receiver gets value of the threshold, receiver will get exact idea of the threshold number of shares. Unreliable waiting of the receiver will not happen. Hence definite, reliable and right data generation takes place.
- Hash value of the message perform role to protect integrity of the secret data.

4.1.1 Detection of malicious route.

Suppose a certain malicious node manipulate the bits of share and forwards it, at receiver side false data is generated. Hence hash value of the message generated will not match. Receiver will compare message hash value to received value. It will know that false data is generated. At this time, receiver will try different combinations of 'k' number of shares. By trying k no. of share combination receiver gets idea of malicious route.

E.g. In the previous mentioned example, suppose share no. 4 is forged.

	0000101001	share 1
OR	0100000001	share 2
OR	1000001001	share 3
OR	1111101000	share 4 (forged by malicious node)
OR	1000100000	share 5
	1111101001	false secret is generated at receiver

At this point by comparing hash value of the messages ,receiver come to know that message generated is false.

Now receiver will try k no. of combinations, k=3. Say receiver may try share 1, 2, 3.

	0000101001	share 1
OR	0100000001	share 2
OR	1000001001	share 3
	1100101001	original data

Now receiver will again compare the hash value of message generated is right. So shares 1, 2, 3 are marked as true.

Now receiver will remove one of the share and try different combination. Say it has removed share 3, and try share 1,2,4.

	0000101001	share 1
OR	0100000001	share 2
OR	1111101000	share 4 (forged share)
	1111101001	false data

But receiver knows that share 1 and 2 are correct. So consequently share 4 must be forged. Hence route assigned for share no. 4 must be malicious. Thus receiver will come to know about malicious route.

4.1.2 Detection of malicious node

It is possible to detect malicious node from the proposed approach (ENSS). Suppose there exist a malicious node in network. Let us consider node B which detects various malicious routes from various senders in various times. Let R be set of different routes detected by node B. Let S_i be the set of nodes on route R_i. Let there are m route detected by node B. If node B performs intersection operation on these sets ,$S_1 \cap S_2 \cap S_3 \cap \ldots. \cap S_m$, node B will get malicious node. Also it can be intersection of combination of 'r' number of S, where $r<m$ i.e.$S_1 \cap S_2 .. S_r$ By this way it is possible to detect malicious node from ENSS approach.

4.2 Random path encryption

4.2.1 Public key encryption

Public key encryption can be one of the way to encrypt the random path. We are assuming some efficient key management scheme viz digital certificates. In cryptography, RSA[10] is an algorithm for public-key cryptography It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently sure given sufficiently long keys and use of up to date implementation. Although public key encryption is more battery driven process, but only one time encryption is providing robust security. So for this cause it is reasonable to use public key encryption.

4.2.2 Symmetric key encryption

In this technique symmetric key is generated securely[11].e.g. In Bluetooth devices the sender and receiver used pass code for authentication purpose. The same idea can be carried out here.

In adhoc networks usually there is human sitting on each node of the network. In the common use case, where two devices are to be used in the most basic ad hoc set-up as suggested, there is usually human presence, which intervenes like a base station. This practical assumption of human presence, at least at initiation, is in line with this basic definition of ad hoc networking. Based on human communication (pass code) algorithm develops symmetric key locally for authenticated communication . There cannot be possibility of any middle man attack.

.

4.3 Overcoming network layer threats

Proposed approach (ENSS) is able to overcome network layer threats such as black hole, gray hole, wormhole, jellyfish attacks. As we are assuming certain loss, we are sending information in multiple shares keeping redundancy. So loss of few shares due to these attacks would not affect the information regeneration. In case of Sybil attack, we are sending shares asynchronously, so time delay in sending phase will not allow Sybil attacker to collect minimum number of reconstructable shares.

5. COMPARISON

Parameter	**NSS**	**ENSS**
Data Transmission	Via multiple paths	Via multiple paths
Computational Complexity	Low	Moderate because of hash creation, one time public key encryption etc
Energy saving	High	Moderate
Detection of Malicious route	Not possible	Possible
Detection of malicious node	Not possible	Possible
Shares transmitted	Asynchronously	Asynchronously
No. of shares received less than threshold	Cannot be verified by receiver	Can be verified by receiver
False secret generation	Yes, there is a possibility	Not possible
Integrity maintained	No	Yes
Confidentiality	High	High
Reliability	Low	High

6. CONCLUSION AND FUTURE SCOPE

The algorithm proposed is extended version of Novel Security approach for overcoming its serious drawbacks. Both approaches based on shared secret cryptography. The proposed approach sends the message parameters, hash value, threshold value securely to receiver. In proposed ENSS approach, it is also possible to find malicious route and possible to have more confidentiality, integrity and authentication. Hence the ENSS approach seems to be more reliable.

Future scope of paper will be scheme should integrate with efficient key management scheme.

7. REFERENCES

[1] Supachote Lertvorrathan, INTEGRATED SECURE MULTIPATH MOBILE ADHOC NETWORK, School of applied Statistics National Institute of Development 2010.

[2] A Novel Security Scheme for Wireless Adhoc Network, Abhijit Das Soumya Sankar Basu Atal Chaudhuri, 978-1-4577-0787-2/11 IEEE 2011.

[3] 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.

[4] “Security issues in MANET”,Rashid Sheikh,Mahakal Singh Chandel,Durgesh Kumar Mishra, 978-1-4244-7202-4/10 IEEE 2010.

[5] 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 1997

[6] Y. Desmedt and Y. Frankel “Threshold cryptosystems” Proc of CRYPTO’89 volume 435 of LNCS, pp 307-315 Springer Verlag 1990

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

[8] G. Blakely : “Safeguarding cryptographic keys “ Proc. of AFIPS National Computer Conference, 1979.

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

[10] Revest R, Shamir A and Adelman L, “ A Method for Obtaining Digital Signature and Public Key Cryptosystem” Communication of the ACM, pp. 120-126,1978.

[11] Authentication in Adhoc Networking,A O Salako, University college , London