International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Reformed Security Scheme for False Node Detection in Wireless Ad Hoc Networks

J. Nithyapriya[1], Dr. V. Pazhanisamy[2]

[1]Research Scholar, Alagappa University, Karaikudi, Tamilnadu, India

[2]Professor and Head, Department of CA, Alagappa University, Karaikudi, Tamilnadu, India

Abstract: ***A "wireless ad hoc network" consists of various mobile nodes connected by wireless links. The union of which makes an arbitrary graph. In a wireless ad hoc network, nodes can openly move around while communicating with each other. Being a network which is able to connect multiple nodes and networks with any large distance security becomes the biggest concern because the information travels through many unknown nodes and multiple paths. Sending information through a single path is not prudent because it can be easily hacked; the single path cannot be fully trusted. To get rid of hacking the sender may send multiple copies of the information through multiple paths. This increases the risk of information leakage. Shared cryptography addresses this concern. Clustering the nodes managestraffic. This paper puts forth a reformed Security Scheme for Wireless Ad hoc Networks to detect malicious nodes by combining the clustering scheme, uncertainty of receiver's authenticity were sensed.***

Keywords: Ad hoc, Arbitrary Graph, Cryptography, Clustering

1. About Ad Hoc Network

Wireless nodes network among themselves even when the access to the internet is unavailable. From instant conferencing between notebook PC users to emergency and military services that must perform during harshest conditions ad hoc helps. Ad hoc networks have a unique set of challenges.

[1] Ad hoc networks face challenges in secure communication.

The resource constraints on nodes like power consumption in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus the susceptibility to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion is high.

[2]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.

[3]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.

2. Literature Survey

Attacks ultimately target the weakness of this kind of network. Security is not a single layer issue but a multilayered one in ad hoc networks. Due to the 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 an 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. The received shares will be reconstructed. This not only reduces the risk of information leakage but also reduces the chance of several possible network level attacks in wireless environment.

3. Novel Security Scheme[1]

In "Novel security scheme for wireless ad hoc networks" 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 and 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. This scheme thus forms the mask of size ${}^{n}C_{k-1}$, which will be repeatedly ANDed over the secret in any regular order because for every bit position there should be ${}^{n}C_{k-1}$ such combinations. Different mask will produce different shares.

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.

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

Step 2: Arrange them in the form of a matrix having 'n' number of columns and each row having 'K' number of 1's.Obvious dimension of the matrix will be nCk-1 × n.

Step 3: Transpose the matrix generated in Step-2. 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

The secret code that is to be sent from node A to node B is 10111100.n=5 and k=3 i.e. the secret code is sent through 5 multiple paths with the threshold value 3.
Mask designing for=5 and K=3 for the secret code 10111100.
Step1: Create row vectors.
[00111] , [01011] ,
[01101] , [01110] ,
[10011] , [10101] ,
[10110] , [11001] ,
[11010] , [11100]
Step2: From a matrix out of the row vectors.

00111
01011
01101
01110
10011
10101
10110
11001
11010
11100

Step3: Take transpose of the above matrix. Let each row be the mask for 'n' different paths.
Mask1:0000111111
Mask2:0111000111
Mask3:1011011001
Mask4:1101101010
Mask5:1110110100

Take AND the secret code and each mask.

Secret: 10111100
Mask1: 0000111111
0000111100 : SHARE 1

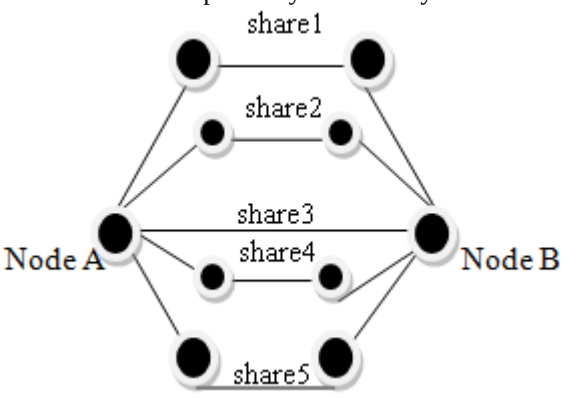
Secret: 10111100
Mask2: 0111000111
0010000100 : SHARE 2

Secret: 10111100
Mask3: 1011011001
0010011000 : SHARE 3

Secret: 10111100
Mask4: 1101101010
0000101000 : SHARE 4

Secret: 10111100
Mask5: 1110110100
0010110100 : SHARE 5

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



Multi path share sending

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

	0000111100	: SHARE 1
OR	0010000100	: SHARE 2
OR	0010011000	: SHARE 3
OR	0000101000	: SHARE 4
OR	0010110100	: SHARE 5
	0010111100	Original message

Even if some shares are missing on the way and only few number of shares reach the receiver, if the number of shares received = K we can always get the secret code because K number of shares is enough to extract the secret code.

	0010000100	: SHARE 2
OR	0000101000	: SHARE 4
OR	0010110100	: SHARE 5
	0010111100	Original message

Drawbacks of NSS

- In NSS value of the threshold is unknown to the receiver - network characteristics may change in future.
- There is no facility of detecting malicious route. The malicious node may manipulate 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
- 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 0000101011 instead of 0000101000. So at receiver side false secret is generated.

	0000111100	: SHARE 1
OR	0010000100	: SHARE 2
OR	0010011000	: SHARE 3
OR	0000101011	: SHARE 4(changed)
OR	0010110100	: SHARE 5
	0010111111	(false secret generated)

Above mentioned serious issues need to be resolved.

4. Enhanced Novel Security Scheme For Wireless Adhoc Networks: Enss [2]

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.

4.2 Detection of Malicious route

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

0000111100 share 1
OR 0010000100 share 2
OR 0010011000 share 3
OR 0000101011 share 4 (forged by maliciousnode)
OR 1000100000 share 5

1010111111 (false secret)

At this point by comparing hash value of the messages, receiver comes 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.

	0000111100	: SHARE 1
OR	0010000100	: SHARE 2
OR	0010011000	: SHARE 3
	0010111100	(Original message)

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 shares and try different combination. Say it has removed share3 and try shares 1, 2, 4.

0000111100 share 1
OR 0010000100 share 2
OR 0000101011 share4 (forged by malicious node)

0010111111 (false data)

4.3 Analysis of ENSS

Detection of malicious node
It is possible to detect malicious node by intersection operation on these sets, $S_1 \cap S_2 \cap S_3 \cap \ldots \cap S_m$, node B will get malicious node. S-set of nodes in route $R_{i..}$

Public key encryption
Public key encryption is more battery driven process. But using public key encryption provides robust security. So for this cause it is reasonable to use public key encryption only once.

Symmetric key encryption
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.

Successful dealing of network layer threats
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. Implementing ENSS in Clustered Environment of Wireless Ad Hoc Networks

These networks build and start with the help of constituent wireless nodes. Since these nodes have only a limited transmission range, it depends on its neighboring nodes to forward packets. A node may be start working selfishly by using its limited resource only for its individual benefit; such selfish nodes cause a wide range of problems .Wireless Ad hoc network is proven to be the top research area with the focuses on security, performance, energy and so on. In the clusters of wireless ad hoc networks the false nodes leads to a big problem as increase congestion. Hence we split wireless ad hoc network into a number of size clusters having a cluster head and storage capability. We find false node inside clusters of wireless ad hoc network with the help of modified false node detection algorithm and try to remove them and also compare the result according to throughput and delay.

5.1 Cluster Creation Algorithm:[3]

```
While (MobileNodeStatus == true)
 {
 For (i=1 to M) //m is total no of nodes.
          {
          Find connectivity degree of Nodes ();
          Find the RSS (); //relative signal strength among
nodes.
          If (connectivity _degree ==THcd && RSS ==This)
          // THcd and This is predefined threshold.
                    {
                    //Create cluster;
                    Add node Ni into cluster Cj;
                    }
          For (Cj= 1 to P) // P is the total no. of clusters
                              {
                               For remaining Nodes
                              {
          If (number of nodes in Cj > S) // S is the size of
cluster in term of no. of nodes.
                                        { j++;
                                             } } } } }
```

ENSS Algorithm in cluster

1) Sender counts the paths in a cluster available for the transmission i.e. it decides the value of n_c
2) The sender decides value of threshold of cluster (k_c).
3) The sender designs the mask according to values of n_c & k_c.
4) The sender applies the mask and generates the shares.
5) Each share of same message is assigned a unique number. The sender sends the shares via multiple disjoint paths.
6) Each path is assigned a number.
7) Among the n_c paths one path is randomly chosen.
8) 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)

6. Conclusion and Future Scope

We have done a detailed study on the prominent security schemes for wireless ad hoc networks. By this study we get known that the key strategies like shared secret cryptography, Public key encryption, Symmetric key encryption are used to attain the some of the key goals of security like confidentiality, integrity and authentication. The other idea behind splitting wireless ad hoc networks into a number of size clusters having cluster head and storage capability as per the cluster formation algorithm given. In our proposal we find false node inside clusters of wireless ad hoc networks using shared cryptography and multipath share sending. Hence we detect false nodes still reducing congestion. In future these schemes may be enhanced to attain high saving of energy and less computational complexity.

References

[1] A Novel Security Scheme for Wireless Adhoc Network, Abhijit Das Soumya Sankar Basu Atal Chaudhuri, 978-1-4577-0787-2/11 IEEE 2011.
[2] Enhanced Novel Security Scheme for Wireless Adhoc Networks: ENSS , Prasad Patil ,Rinku Shah ,Kajal Jewani, International Journal of Computer Applications® (IJCA) ,2012
[3] An Approach: False Node Detection Algorithm in Cluster Based MANET, Gaurav, Naresh Sharma Himanshu Tyagi , Volume 4, Issue 2, February 2014

ISSN: 2277 128X ,International Journal of Advanced Research in Computer Science and Software Engineering
[4] Acknowledgment-Based Secure authentication Method for Manet by Dr.J.Subash Chandra Bose et al.,IJIRCCE, March 2014.
[5] An Approach: False Node Detection Algorithm in Cluster Based MANET , IJARCSSE ,Gaurav, Naresh Sharma, et al., February 2014.
[6] Improved Adaptive Acknowledgement Scheme For Intrusion Detection System In Adhoc through SCADA by G.Dharma prabha et al., *IJCSITS, December 2014.*
[7] "Security issues in MANET",Rashid Sheikh,Mahakal Singh Chandel,Durgesh Kumar Mishra, 978-1-4244-7202-4/10 IEEE 2010.