Enhanced Secure Protocol for Reliable Data Delivery

T. Srinivasa Rao
Department of Computer Science
Lovely Professional University

Gagandeep Singh
Department of Computer Science
Lovely Professional University

ABSTRACT
We are providing the concept of securing the data in the MANET environment to get the high confidentiality rate while transferring the data in the network. The Enhanced SPREAD is a concept of transforming the data into the network by dividing the secret message into multiple data parts by taking the help of secret sharing algorithms that are presented to provide High security to data by optimal encryption technique. Here we are providing the entire architecture and three major issues that are present in the MANET. First issue is how to get the data parts by using the secret sharing method, Secondly by allocating the data shares onto each path should be in the optimal way so that security can be increased. Coming to the third issue, this depends on the routing protocol and multipath routing techniques in MANET.

General Terms
Blowfish block cipher algorithm.

Keywords
Routing, Network security, Ad hoc networks.

1. INTRODUCTION
MANET (Mobile Ad-hoc Network) is a challenging technology that we are using from past few years. A MANET is wireless and infrastructure less network with broadcast nature. This network supports many properties like self-organizing, self-configurable and tactical network. Nodes that are present in the network are called as hops by this; we can also call MANET as a multi hop network. Every node in the MANET contains the property of discovering the neighboring nodes, maintaining the network and forwarding and receiving the data packets. MANET is an infrastructure less network because each node in the network is movable (called mobile nodes) at any point of time this causes a topology change in the network. Due to the infrastructure less property this can be used in the military applications like communication among the soldiers in the battle field also at the earth quake rescue operations. Due to properties of the wireless and infrastructure less nature we can say this is not a reliable network.

There are few attacks that are present in the MANET to access the confidential data that is passing through the network the attacks are DOS (Denial of Service) and Eaves Dropping. Providing security and managing key is very important because data can be compromised by the unauthorized persons.

2. RELATED WORK
The important issue in the MANET is security. While comparing wired and wireless environments, security is always less in the wireless environment because of broadcasting in nature and unreliable networks. The security applications which we are using in the wired environments may not be applicable in wireless environments, such as MANET. There is a lot of research work that is going on providing security in MANET. There are two major issues that are present in the MANET regarding security those are Key management and Secure routing protocol.

Managing the key in the ad-hoc environment is very typical issue. The services those are dealing with the cryptography like confidentiality and authentication depend only on key the management. Certification Authority (CA) is generally responsible for managing the keys in wired environment. Coming to our Enhanced SPREAD we are dealing with different encryption keys those are physically independent. Key management is done by local neighbor nodes.

Selection of routing protocol contains many steps because data is sending through this routing path. Selecting the secure routing protocol is to protect the data from hackers. This routing path must be highly secured, which is dealing with the node failures, compromised nodes and disjoint nodes. Here we are going with the disjoint path set selection protocol (DPSP) to detect the more edge-disjoint paths that are presented in network.

3. ENHANCED SPREAD OVERVIEW
3.1 System Model
The idea for this Enhanced SPREAD comes for the observation. While we are transferring the data through the network it may be captured by any intruder. Then this may cause loss of information or revealing the secrecy in data. Our Enhanced SPREAD deals with same process while source node sending data to the destination node then source node initially select the multiple paths that are used to reach the destination by using multipath routing. This also considers some properties like disjoint nodes. Then source node selects the threshold secret sharing algorithm. Based upon the security level of the data the sources node adjusts the data parts on to the multiple paths and send those to the destination. Upon receiving multiple data parts by receiver node then receiver can adjust data by Threshold secret sharing algorithm.

We are dealing with the key management by the neighbor nodes. Intruder may capture the message, which is traveling through the particular node. Once the node is decrypted by the intruder then entire data which is passing to that node will be captured and then intruder will rebuild the original message. Here we mainly focused on the three major design issues in the MANET. This is depends on the cryptography, optimization and the network routing. In this particular scenario, cryptography deals with dividing large data into multiple data parts, optimization deals with, how these data parts have to put on the multiple paths and finally network routing deals with, how to select these multiple paths. This E-SPREAD gives optimal solutions for three issues that are presented in the MANET. Those are security, reliability and cost metric. Each of the issue that is presented in E-SPREAD is explained in the following sections.

3.2 Threshold Secret Sharing

The primary issue in the Enhanced SPREAD is that how to divide the data into multiple data parts or pieces. Dividing the big message into few small segments will not provide any security because every data part contains some information. The message integrity need some extra protection for this purpose we are using (T, N) Secret Sharing scheme.

This (T, N) Secret sharing scheme divides the secret data message into N parts or shares and in order to compromise the data by the hacker needs at least T shares. Each share holds some secret information. Less than T shares the intruder doesn't learn anything from the share which it contains. The intruder doesn't get any information from the share it contains. Reconstruction of the message is based upon the linear operations over the minimum fields. Consider an example of Shamir's Lagrange interpolation polynomial scheme; this is a secret sharing scheme that also detects deceitful detection and identification. Identification of these cheating nodes is not a matter in our paper this only helps for integrity of the data that is transmitted.

3.3 Share Allocation

Here there is a second issue; this is dealing with how to allocate the data parts on each path that are selected. Allocation of the data part on the correct path is very important if intruder compromises any node then all the data that is passing via node can be compromised. So that initially selects the paths according to their security properties and allocates the data share according to the security onto paths. Allocate one data part on the each path. This process increases the security of the data. The intruder has to compromise N number of paths to get the data. By applying (N, N) secret sharing and allocate one data part to each path this will gives maximum security with less cost metric.

MANET is an infrastructure less network the topology may change at any point of time. Due to the change in the topology the packets may loss during the transmission. If some data parts are lost by the topology change the reconstruction of the data message can be done at the destination side. To do the reconstruction of the message at the destination side it must contains T shares out of N shares (i.e., T<N). By using the (T, N) security scheme we can add more reliability and redundancy to the Enhanced SPREAD without scarifying the security.

3.4 Multipath Routing

The final issue, which we are discussing in this E- SPREAD is that how to find multipath in MANET to deliver the message from source node to the destination node. Routing in the Mobile ad-hoc network is very difficult because nodes in this network are not stable. Due to the mobility of the nodes the topology may change at any point of time. Multi path routing is a difficult routing technique to deliver the data. Distributing the data on to the nodes will decrease the battery consumption. For E-SPREAD we required many independent paths, because we are facing with the problem of node compromise. Especially we require node-disjoint paths to avoid from the above node compromising problems. There are many routing protocols are presented in MANET to deal with this problem for example split multipath routing, on-demand routing and dynamic source routing. On-demand routing protocol is capable for maintaining multiple paths from source node to destination node.

The path selection in this routing is based upon the hop count and propagation delay by using the on-demanding and source routing type of approach to Enhanced SPREAD. Using the "link cache" organization where each path returned to the source is festering into individual links and displayed as data structures. This "link cache" organization is useful for viewing the network topology partially. To provide the better security for data delivery we have to use maximal node-disjoint path algorithm to get multiple node-disjoint paths.

4. MESSAGE SHARE GENERATION

The brief explanation of the Threshold Secret Sharing is given in this section. This is required to make the data into multiple data parts. Let's consider secret of the system is K and we divided the entire data in to N number of parts and we also called them as shares. The shares are *S1, S2, S3 . . . , SN.* All the paths holds one share each respectively, those are like P1, P2, P3 . . . , PN. This algorithm divides the shares according to its theory that fewer than T shares will not give any information to the intruder. The data parts which are T out of N can use to reconstruct the secret data K. This process is known as (T, N) Threshold Secret sharing scheme.

This scheme contains two algorithms known as dealer and combiner. The dealer at the source side is used to divide the data into multiple parts and allocates them in to different paths. And the second algorithm combiner is used to gather the data parts from the paths and reconstruct the message from the K secret and from the T data parts received at the destination. The combiner will only re-compute the data message if and only if it got T data parts.

Here is the Enhanced SPREAD we are using the Shamir's Lagrange interpolating polynomial method. This is one of the secret sharing methods. The source node initially gets the i^{th} path i.e., Pi's share Si by processing a polynomial degree (T-1).

$$f(x) = (K+d1x+d2x2+dT\text{-}1xT\text{-}1) \bmod p$$

$$at\ x = i\ (i=1, 2, 3, \ldots, N):$$

$$Pi\ Si = f(i)$$

Here *d1,d2,…,dT-1* are randomly selected coefficients, also p is randomly taken prime number which is larger than the all other coefficients and this must be presented with both dealer and combiner. The secret of the message K is also denoted with the coefficient "a0". At the destination side (combiner), by taken the T data parts, *f(i1),f(i2),…,f(iT),* the original data f*(x)* can be recover by the Shamir's Lagrange interpolation.

$$F(x)=\sum_{J=1}^{T} S_{ij}.l_{ij}(x) \bmod p$$

Where

$$l_{ij}(x)=\prod_{k=1,k\neq j}^{T} x\text{-}i_k \,/\, i_j\text{-}i_k$$

Larger the (T, N) will not be more in our Enhanced SPREAD technique. For the practical implementation of Enhanced SPREAD, the straight forward quadratic algorithms are quite enough. The secret share of the can be applied as block-by-block. This is a basic and fundamental technique is to perform encryption to the data. Here in the Enhanced SPREAD technique we are using the Blow Fish Algorithm (BFA) to

protect the data from the intruders and to hide the original message.

The bandwidth is the basic constraint in the wireless networks. The bandwidth is to be reduced in this wireless environment. To reduce the bandwidth in our Enhanced SPREAD more and more coefficients has to be allocated to the data parts or data blocks. Those are *d0,d1,d2,…,dT-1*.

5. OPTIMUM SHARE ALLOCATION

Here in the Enhanced SPREAD the main constraint is the security. Providing the security to the data is our main aim for the security purpose we are using (T, N) secret sharing algorithm. The network layer is mainly responsible for transferring the data from one hop to another hop. The network layer is to find the disjoint nodes in the route initially to protect the data more. If any disjoint node is compromised then every data that -is traveling from that disjoint node can be compromised.

Let us consider there are "M" disjoint paths that are present in the network. Denoted with the vector "p' i.e., p=[p1,p2,p3,…..,pM] and security characteristics are denote to this paths is with pi, [i=1,2,….M]. pi are the nodes that says the probability of compromised nodes.

If the N=T then the original data can be easily recovered from the T shares of the data. If (N>= M) or N=N then the data is fully secured i.e., maximum security is assigned. Here we are using the Blow Fish block cipher encryption algorithm which is more advanced algorithm which uses 64 bit block size and variable key size up to 448 bits long.

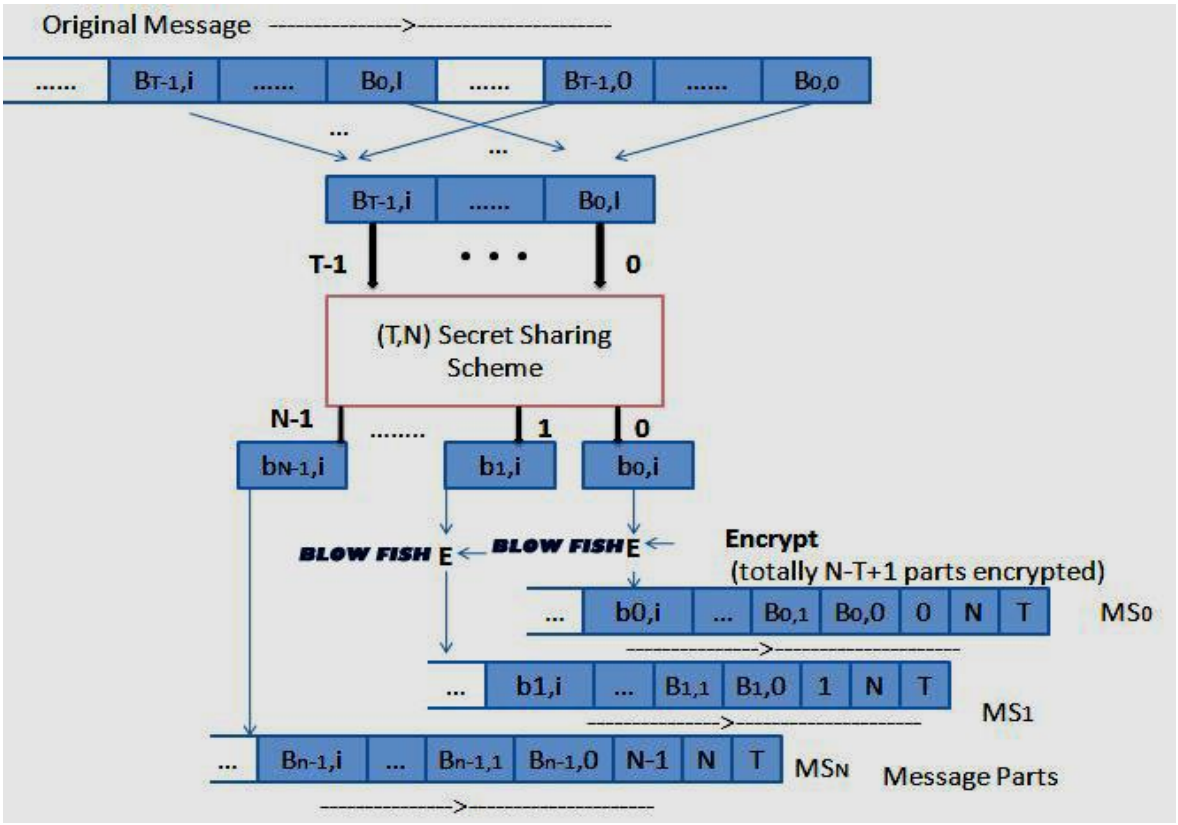

Fig 1: (T, N) Secret Sharing Scheme using Blowfish Encryption

6. MULTIPATH ROUITNG

The main challenge in the ad-hoc network is routing. This routing carries many functions those are nodes should be properly connected, the data should be delivered correctly to the destination node, malicious node should be identified, routing information should be updates every time and must handles the disjoint nodes in the network. Here in our Enhanced SPREAD we are using the multipath routing protocol named as on-demand routing protocol which is very effective and efficient routing protocol in the ad-hoc environment. The on-demand routing protocol is also used to handle the disjoint nodes in the network. Which is also maintains the link cache organization to update the route and also to gives the reply to the source node time to time. This link cache is maintains the minimum hop count and minimum propagation delay.

Here we also use the Dijsktra's shortest path process to get the minimum hop count. Here source node initially enters the destination node ip-address then broadcasts the data to its neighboring nodes. All the remaining nodes that are presented in the networks handle this task to deliver the data to the destination node. If any node is failed in the network then the previous node from the failed node will select another route to the destination.

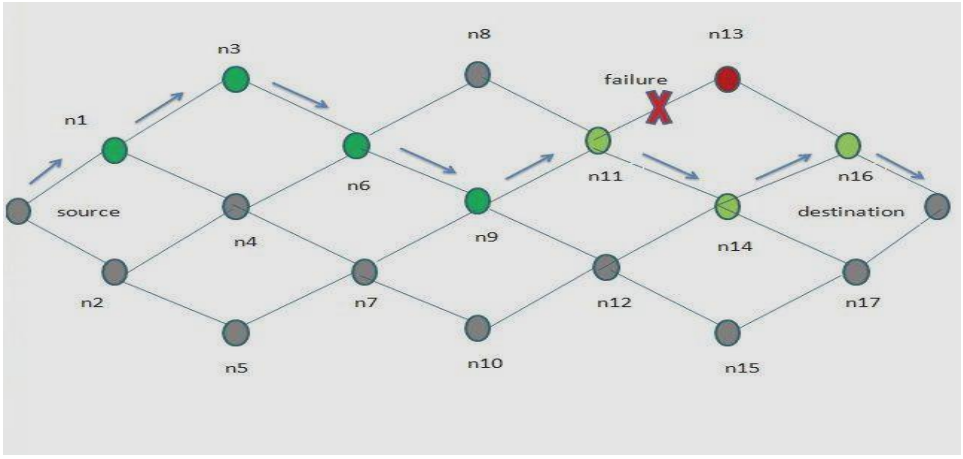

Fig 2: Multipath Routing In E-SPREAD

7. CONCLUSION

Here in the Enhanced Security Protocol for Reliable Data Delivery (Enhanced SPREAD). We are using the most recent and powerful block cipher algorithm named as Blow Fish Algorithm which gives good result than the previously implemented block ciphers. Here in the Enhanced SPREAD we are dividing the data in to multiple shares and then we are passing it to the (T, N) secret sharing scheme which gives more security to the data and if the intruder compromises the small blocks also cannot understand the entire data. These data blocks are transferred through the multipath on-demand routing protocol. This Enhanced SPREAD will give more secure data delivery from the source node to the destination node in the mobile ad-hoc networks environment.

8. REFERENCES

[1] Wenjing Lou, Wei Liu, Yanchao Zhang, Yuguang Fang, SPREAD: Improving network security by multipath routing in mobile ad hoc networks. [2012]..

[2] Ankur Lal, Dr.Sipi Dubey, Mr.Bharat Pesswani, Reliability of MANET through the Performance Evaluation of AODV, DSDV, DSR.CSE, CSVTU [2012].

[3] Shamir, How to Share a Secret, Communications of the ACM. (Nov 1979).Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] J.W. Suurballe, Disjoint paths in a network, Networks 4 (1974).

[5] Schneier, Bruce. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)." Blowfish" Paper. 1993. Web. 18 Mar. 2012.

[6] T. Cormen, C. Leiserson and R. Rivest, *Introduction to Algorithms* (MIT Press, 1990).

[7] T.-C. Wu and T.-S. Wu, Cheating detection and cheater identification in secret sharing schemes, IEE Proc. Comput. Digit. Tech.142(5) (September 1995).

[8] W. Lou and Y. Fang, Predictive caching strategy for on-demand routing protocols in ad hoc networks, Wireless Networks 8(6) (Nov 2002).