International Journal of Science Engineering and Advance Technology

A new Security approach for integrating wireless adhoc network using octant bit computation and routing test

Sushmita Silwal[1] ,Anu Sharma [2]

TMU University, Moradabad, Uttar Pradesh, India

[1]sushmitasilwaliftm@gmail.com

[2]er.anusharma@gmail.com

***Abstract*— Ad hoc networks are a kind of network that has no centralized body and in order to communicate with the nodes it has no fixed topology.In this paper we propose to use binary masking of octant bits and shared cryptography to secure message communication in ad-hoc network and we have proposed a minimized computational security scheme for wireless ad-hoc network based on shared information between source host and destination host .We also can focus on routing test before transferring packet because , no of packet increases due to binary masking technique. With the help of this method we make the virtual path between source and destination. 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— Ad-hoc Network, Security threats, virtual path, computational.

Introduction

The specific network nodes which are constructed and organized for establishing the dedicated pathways for efficient routing of data between the user and the desired destination are called adhoc or mesh networks. For making the transmission of information safe and secure, it is must to implement some security mechanism within the wireless adhoc communication network. The shared wireless medium and the diversed co-ordination meshanism make these wireless networks more unsafe and unsecure for ciber/digital attacks than traditional wired networks where the central co-ordination mechanism and unshared medium access minimize the attacking probability. The wireless adhoc networks can be affected by number of attacks. Generally these attacks can be classified into two types:-

Physical layer attacks

Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers. The mobile hosts in mobile ad hoc networks share a wireless medium. The majorities of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency [7] [4]. Thus, messages transmitted can be eavesdropped, and fake messages can be injected into network. Moreover, a radio signal can be jammed or interfered, which causes the message to be corrupted or lost [7]. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse. Jamming equipment is readily available. In addition, jamming attacks can be mounted from a location remote to the target networks.

Link layer attacks

The adhoc is an open mulitpoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbors is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols.

Performance

Throughput and Overhead

The watchdog and pathrater mechanism with DSR algorithm improves throughput by 27% while increasing the overhead from 12% to 24%. But this overhead is due to the way DSR operates to maintain routes. The watchdog itself adds very little overhead. Although the overhead is significant, these extensions still improve net throughput. In networks with moderate mobility throughput improves by 17% while overhead transmission increases from 9% to 17%.

Security-awarded-hoc routing(SA)

It makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Current routing protocols discover the shortest path between two nodes. But SAR can discover a path with desired security attributes (E.g. a path through nodes with a particular shared key). A node initiating route discovery sets the sought security level for the route i.e. the required minimal trust level for nodes participating in the query/ reply propagation. Nodes at each trust level share symmetric encryption keys. Intermediate nodes of different levels cannot decrypt intransit routing packets or determine whether the required security attributes can be satisfied and drop them. Only the nodes with the correct key can read the header and forward the packet. So if a packet has reached the destination, it must have been propagated by nodes at the same level, since only they can decrypt the packet, see its header and forward it.

Previous work

THRESHOLD CRYPTOGRAPHY:-

Threshold Cryptography is the art of chopping a secret into little bits. Only by possessing more than a threshold number of bits of the secret can the secret be determined. For example if I had four copies of a key and cut each key into three pieces, distributing one piece each to twelve people then it would probably take about five people to use the key. The minimum threshold in this case would be three, and the maximum number of servers to contact would be 9. That's with random distribution. With algorithmic, non-random distribution based on name (e.g. the four lowest in the alphabet get piece1, the next four get piece2, etc.), this can be reduced to exactly three successful contacts necessary to find the whole key. 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 based on polynomial interpolation, Blakley based on hyper plane geometry and Asmuth-Bloom 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 binary masking for share generation and reconstruction can be done by simple ORing 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.

POLYNOMIAL INTERPOLATION:-

In numerical analysis, polynomial interpolation is the interpolation of a given data set bya polynomial: given some points, find a polynomial which goes exactly through these points. Polynomials can be used to approximate more complicated curves, for example, the shapes of letters in typography, given a few points. A relevant application is the evaluation of the natural logarithm and trigonometric functions: pick a few known data points, create a lookup table, and interpolate between those data points. This results in significantly faster computations Polynomial interpolation also forms the basis for algorithms in numerical quadrature and numerical ordinary differential equations A theory of polynomial and rational matrix interpolation is introduced in this paper and its application to certain Systems and Control problems is discussed at length. Note that many system and control problems can be formulated in terms of matrix equations where polynomial or rational solutions with specific properties are of interest. It is known that equations involving just polynomials can be solved by either equating coefficients of equal power of the indeterminate or equivalently by using the values obtained when appropriate values for s are substituted in the given polynomials; in the latter case one uses results from the theory of polynomial interpolation. Similarly one may solve polynomial matrix equations using the theory of polynomial matrix interpolation presented here; this approach has significant advantages and these are discussed below. In addition to equation solving, there are many instances where interpolation type constraints are being used in systems and control without adequate justification; the theory presented here provides such justification and thus it clarifies and builds confidence into these methods. Polynomial interpolation has fascinated researchers and practitioners alike. This is probably due to the mathematical simplicity and elegance of the theory complemented by the wide applicability of its results to areas such as numerical analysis among others. Note that although for the scalar polynomial case, interpolation is an old and very well studied problem, only recently polynomial matrix interpolation appears to have been addressed in any systematic way . Rational, mostly scalar interpolation has been of interest to systems and control researchers recently. Note that the rational interpolation results presented here are distinct from other literature results as they refer to matrix case and concentrate on fundamental representation questions. Other results in the literature attempt to characterize rational functions that satisfy certain interpolation constraints and are optimal in some sense and so they rather complement our results than compete with them.

HYPER PLANE GEOMETRY:-

In this work, we show how to do threshold RSA signatures using Blakely SSS. Blakely's scheme, which is based on solving linear systems, naturally requires computing inverses for reconstructing the secret. We show, in a spirit similar to Shop's work, how to utilize Blakely's SSS for threshold cryptography while avoiding computation of inverses modulo _ (N) completely.

An anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks was proposed in [5]. Based on a new cryptographic concept called pairing, an anonymous neighbourhood authentication protocol which allows neighbourhood nodes to authenticate each other without revealing their identities was suggested. The secret pairwise link identifiers and keys established between

neighbours were utilized during the neighbourhood authentication process. MASK fulfils the routing and packet forwarding tasks nicely without disclosing the identities of participating nodes under a rather strong adversarial model. It also provides the desirable sender and receiver anonymity, as well as the relationship anonymity of the sender and receiver. It is also resistant to a wide range of adversarial attacks; moreover, it preserves the routing efficiency in contrast to previous proposals.

PROPOSED FRAMEWORK

Binary masking (new technique)

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 communicating nodes. 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 computational overhead in our scheme is substantially low as it employs elementary graphical masking method, done by simple binary masking for share generation and reconstruction can be done by simple ORing the qualified set of shares. 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 our scheme. 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.

A unique non-zero identification number is used to identify each node. All nodes within the network are awared with the knowledge of the total number of nodes at bigining and all non-malicious nodes are kept as the starting network nodes. There exists a route between all pairs of nodes within the network and bi-directional communication between the nodes takes place using this route. Between two pair of nodes, there are multiple numbers of routes available. 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.

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. The data which are in binary form ,the main challenge is how to create there mask here we going to introduce a new algorithms to design mask of binary data the name of that algorithms is binary masking In this algorithm we are working on a binary data with 10 bit

Mask Designing Technique

Steps of binary masking:

First of all take 10 bit binary data as input. After taking input store it into an array and find all array addresses with zero (0) and one (1) value. After it store all addresses with value one(1). Than change any two addresses with value one (1) to zero (0) and get random bit data of 10 bit length (there is only two bit change from previous data). After it apply circular sift right keeping fix the addresses having value zero (0) and print all possible binary mask (after applying circular sift right).

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. n, 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.

RESULT ANALYSIS

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. Binary masking technique is a new pattern to design mask, by this technique we are able to design mask related to that data as we know that there is no any specific pattern to design masking, but binary masking provide good algorithms to produce Binary mask. In this algorithm we are taking 10 bit length data because in this case the value of n and k equivalent, which gives high performance.

CONCLUSION AND FUTURE WORK

In this paper we have proposed a security scheme for wireless ad-hoc network with minimal computational complexity 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. In future we can also include credibility management and routing test procedure which provide identification of malicious nodes, when we successfully identify malicious node then we can easily leave those nodes for the selecting path from those node.

References

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

[2] 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, 2002

[3]Abhijit Das, Soumya Sankar Basu ,Atal Chaudhuri" A Novel Security Scheme for Wireless Adhoc Network 978-1-4577-0787-2/11/$26.00 ©2011 IEEE

[4]Li pengweiTeaching department of computer of Anyang normal university, Xu zhenqiang College of information science and engineering of He'nan university of technology" Security Enhancement of AODV against Internal Attacks, 978-1-4244- 7618-3 /10/$26.00 ©2010 IEEE

[5] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.

[6] Sukla Banerjee , "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,"Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[8] Nishu Garg and R.P.Mahapatra, "MANET Security Issues ," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[9] N.Shanthi, Dr.Lganesan and Dr.K.Ramar , "Study of Different Attacks on Multicast Mobile Ad hoc Network," Journal of Theoretical and Applied Information Technology.

[10] V. Madhu Viswanatham and A.A. Chari, "An Approach for Detecting Attacks in MobileAdhoc Networks ," Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008Science Publications.

[11] Hoang Lan and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks", Proceedings of ICNICONSMCL'06, 0-7695-2552-0/06@ 2006 IEEE.

[12] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt,Octomber 2002.

[13] P. Papadimitratos and Z.J.Haas, "Securing the Routing Infrastructure", IEEE Communications, vol. 10, no. 40. Octomber 2002, pp. 60-68. 10] C. PerkinsAd hoc On-Demand
Distance Vector (AODV) Routing RFC3561[S] 2003-7.

[14] Zhu Daofei, Wang Dongyan, Liu xinran. Secure Routing Protocols for ad hoc Networks: a Survey[J]. Computer Engineering and Applications, 2005,(27):116-119.

[15]. Mahendra Kumar* Ajay Bhushan Amit Kumar" A Study of wireless Ad-Hoc Network attack and Routing Protocol attack" International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X Volume 2, Issue 4, April 2012

[16]. Attend Seminor and represented topic "a review on preventing aodv from black hole attack".

[17]http://www.cnsr.ictas.vt.edu/publication/INFOCOM05_Zhang.pdf