Available online at www.pelagiaresearchlibrary.com

Pelagia Research Library

Advances in Applied Science Research, 2011, 2 (4):177-186

Pelagia Research Library
ISSN: 0976-8610
CODEN (USA): AASRFC

Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks

G. S. G. N. Anjaneyulu*, V. Madhu Viswanatham and B. Venkateswarlu*****

**Division of Applied Algebra, SAS, VIT University, Vellore, India*
***School of Computing Science and Engg, VIT University, Vellore, India*
****Dept. of Computer Science, Priya Darshini College of Engg., Nellore, India*

ABSTRACT

Non-infrastructure networks are most commonly called as Mobile Ad hoc networks (MANETs). Unavailability of infrastructure or complexity and expensiveness of setting up the infrastructure results in the need of MANETs. MANETs can also be used when a network is to be setup quickly. The most important and complex problems in this kind of applications are routing, security and key management. The fundamental problem is how to deliver the data packets among nodes confidentially and efficiently without a predetermined topology or centralized control in the unsecured MANET. In this paper, we have given a notion to transmit the data through multipaths between nodes in ad hoc network to enhance the robustness of data confidentiality by secure authentication using digital signature concept.

Keywords: Multipath routing, Digital Signature, MANET.

INTRODUCTION

NETWORKS

In any modern network, there is aneed for security. However, the current internet environment without integrating with security mechanisms has a number of security problems and lacks effective protection and integrity of data transferred over the network below the application layer. The networking communication will be exposed to all kinds of attacks in such an open hostile environment.

Mobile ad hoc networks are self organizing network architectures in which a collection mobile nodes with a wireless network interfaces may form a temporary without the aid of any established infrastructure or centralized administration. According to the IETF definition, a

mobile ad hoc network is an autonomous system of mobile routers connected by wireless links. This union forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily. Thus the wireless network topology may change rapidly and unpredictably.

During the last decade especially at its end, many breakthroughs have been achieved due to fast growing internet. Increased usage of personal computers and mobile phones caused necessity in sharing of information between computers. Establishing static, bi-directional links between computers and performing administrative tasks by the user makes sharing of information difficult to achieve. This complexities lead to construction of temporary networks with no wires, no communication infrastructure and no administrative intervention requirements. Such interconnection between mobile devices is called as Mobile Ad hoc Networks. In such environments mobile devices may take the help of other computers in forwarding the packets to the destination as the transmission range for each mobile host is limited.

Advancements in wireless communication technologies have led to tremendous increase in the usage of small size, high-performance computing and communication devices,. Achievements of second generation mobile system created interests in the field of wireless communications. There are two types of wireless networks; they are infrastructure networks and non-infrastructure networks.

There is no obvious distinction between the two kinds of networks mentioned earlier. The first type is used widely today. It is a wireless network built on the top of a wired network and thus creates a reliable infrastructure network. The wireless nodes act as bridges in a wired network. Wireless nodes are called as base-stations. The best example for this kind of networks is cellular phone networks where a phone connects to the base-station with best signal quality. When a phone moves out of range of a base-station, it does a “hand-off” and switches to a new base-station within reach. The “hand-off” should be fast enough to be seamless for the user of the network.

The second type is Ad hoc network, which does not depend on any stationary infrastructure. All nodes are mobile and can be connected dynamically in an arbitrary manner. In this kind of networks each node serves as a router and participates in the discovery as well as maintenance of routes to other nodes. Router is defined as an entity which determines the path that has to be used to forward a packet towards its final destination. The router selects the next node to which the packet is to be forwarded depending on its current understanding of the state of the network.. Only After advancements in internet infrastructure and micro computer revolution, the packet network ideas became fully feasible and applicable.

Security Requirements in MANET

The most distinct feature of MANET from other static networks is the fact that, in making up routes from various sources to destinations or group of nodes acting as destination is that each node of the network contributes. This distinct feature poses a number of serious threats to the security and privacy of the network as well as the individual nodes making up the network. The directness of Ad hoc networks offers greater flexibility in terms of functionality, but it also provides an open path for any malicious node or hacker to gain access to the network and

perform activities such as eaves dropping, spoofing, denial of service attacks, flooding, link failure etc. Some of the minimum constraints should be met to ensure safe operation of an Ad hoc network are

i). Authentication of a node is very important so that the node can trusted as a trusted node and it is valid, and malicious. Eaves dropping nodes are denial access into the network and
ii). Data integrity is an important issue, so as to ensure the data communicated between nodes has not been altered by any malicious node.

Confidentiality is also necessary, to ensure that no intermediate node can access the data that is meant for the destination of that message.

2. RELATED WORK

Several multipath proactive routing protocols were developed which use table-driven algorithms to compute multiple routes. But they do not consider the power aware metrics and these protocols generate excessive routing overhead and perform poorly in mobile networks because of their proactive nature.

In MANET on-demand routing is most popular one. Instead of periodically route tables of full topology, the on demand routing protocols build routes only when a node needs to send a data packet to a destination. Dynamic Source Routing (DSR) and Ad hoc On demand Distance vector routing are the standard protocols used, but these protocols do not support multipart.

Several multipath on-demand protocols have been proposed recently, some of which being Ad hoc On demand Multipath distance vector(AOMDV) which is an extension to the AODV protocol of computing multiple loop free and link-disjoint paths. The Split Multipath Routing is a Multipath source routing protocol which builds multiple routes. The multi path source routing extends the on-demand DSR protocol. It consists of the scheme to distribute traffic among multiple routes in a network. The Ad-hoc on demand distance vector multi path routing (AODVM) extends ad-hoc on demand distance vector (AODV) for finding multiple node disjoint paths.

The issue of security is addressed by proposing number of advanced protocols which solves the security problems to some extent. The authenticated routing for ad-hoc networks ARAN protocol proposed is a standalone solution for securing routing in ad-hoc networking environments. Cryptographic certificates are used by ARAN in order to achieve security goals of authentication and non-repudiation. The secure routing protocol has a set of security extensions that can be applied to any ad-hoc routing protocols that utilizes broadcasting as its routing querying method [14]. It is specifically mentioned by the author that the DSR is an appropriate for incorporating their proposed security extensions.

The secure efficient ad-hoc network distance vector (SEAD) is a secure ad-hoc network routing protocol which is based on the design of the destination sequenced distance vector (DSDV) algorithm. The distance vector routing protocols utilize a distributed version of bellman ford algorithm in order to find shortest path. To authenticate top count and sequence numbers the SEAD routing protocol employs the hash chains. The Ariadne is a secure on demand protocol

based on DSR and security in the Ariadne follows an end to end approach, while hop by hop security mechanism is followed by SEAD protocol dew to the distance vector routing philosophy it adopts.

The secure ad-hoc on demand distance vector (SAODV) is a proposal for security extension to AODV protocol. In order to secure the AODV packets the proposed extensions utilize the digital signatures. Cryptographic signatures are used for authenticating the non mutable fields of the messages while a new one way hash function is created for every rout discovery process to secure the hop count field in particular, which is the only mutable field in an AODV message. The secure link state routing protocol(SLSP) has been proposed to provide secure proactive routing for mobile and ad-hoc networks. It also secures the discovery and the distribution of link state information both for locally and network wide scope topologies.

The CONFIDENT protocol consists of set of extensions to DSR it includes the following components monitor, reputations system, the path manager and task manager. Security aware ad-hoc routing is an approach to ad-hoc routing that introduces security metric in the route discovery and maintenance operations, treating security routing as a QoS issue.

In 2003, Souheila et.al [2] proposed an general alogorithm in 14th IEEE conference to provide authentication in data transmission using multipath routing. We applied and verified this algorithm to the following signature scheme, which is based on non-commutative division semirings by polynomial symmetrical decomposition problem.

3. SIGNATURE SCHEME

In this paper, the main attention is on transmitting a message/data using in multipath routing by providing secure authentication. So in this section we use the digital signature scheme which was proposed by one of the authors of this paper. Its detailed description is explained in [1], for our convenience, briefly it is given below.

4.1 Semiring

A Semiring R is a non – empty set, on which the operations of addition & multiplication have been defined such that the following conditions are satisfied.(i).(R + 1) is a commutative monoid with identity element ‘O’ (ii) (R .) is a monoid with identity element 1 (iii)Multiplication distributes over addition from either side (iV) 0.r = r.o. for all r in R

4.2 Division Semiring

An element r of a semiring R, is a “unit” if and only if there exists an element r^1 of R satisfying $r.r^1 = 1 = r^1.r$. The element r is called the inverse of r in R. If such an inverse r^{-1} exists for a unit r, it must be unique. We will normally denote the inverse of r by r. It is straightforward to see that, if r & r1 units of R, then $r.(r^1)^{-1}=(r^1).r^{-1}$ & in particular $(r^{-1}) = r$

We will denote the set of all units of R, by U ®. This set is non empty since it sontains “1” & is not all of R. since it does not contain ‘O’. We have just noted that U(R) submonoid of (R, .) which is infact a group U (R) = R {O} then R. is a division semiring.

4.3. Polynomials on division semiring

Let (R, + , .) be a non commutative division semiring let us consider positive integral co-efficient polynomials with semiring assignment as follows. At first, the notion of scale multiplication over R is already on hand. For $k \in Z_{>0}$ & $r \in R$ Then

(k) r = r+r+r+… + r+r (k times)

For k=o it is natural to define. (k) r=O

Property1: $(a)r^m.(b)r^n = (ab)r^n.(a)r^m$, a,b,m,n.€Z, rER

Remark: note that in general (a)r.(b)s # (b)s.(a)r when r # s,since the multiplication in R is non-commutative

Now, let us proceed to define positive integral coefficient semiring polynomials. Suppose the

$f(x)=a_0 + a_1 x + a_1 x^2 +\ldots\ldots + a_n x^n \in Z_{>0}[x]$

Is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R & Finally we obtain.

$f(r)=a_0 + a_1 x + a_1 x^2 +\ldots\ldots + a_n x^n \in R$ *and* $h(r)=b_0 + b_1 x + b_1 x^2 +\ldots\ldots + b_n x^n \in R$

for some $n \geq m$. then we have the following

Theorem l: f(r) .h(r)=h(r) for f(r), h(r) € R

Remark: if r&s are two different variable in R, then f(r).h(s) $\neq$ h(s).f(r) in general.

4.4 Cryptographic assumption on Non commutative division semirings

Let (R, +, .) be a non – commutative division semiring for any a € R we define the Set $P_a \Delta \{ f(a) / f(x) \in z_{>0} [x] \}$

Then let us consider the new versions of GSD and CDH problems over (R.)with respect to its subset P and name them as polynomial symmetrical decomposition (PSD) peoblem and polynomial Diffe-Hellman (PDH) problem respectively.

Polynomial symmetrical decomposition (PSD) problem over Non-commutative division semiring R:

Given (a x, y) € R^3 and m,n € Z, find z € P_a such that $y = z^m x z^n$

4.5. Signature scheme from non-commutative division semirings:

The digital signature scheme contains the following main steps.

4.5.1 Initial setup:

Suppose that (S. +, .) is the non commutative division semiring & is the underlying work fundamental infrastructure in which PSD is intractable on the non-commutative group (S, .) Choose two small integers m, n € Z. Let H: S → *m* be a cryptographic hash function which maps S to the message space M. Then, the public parameters of the system would be the tuple. <S.m,n,M,H>

4.5.2 Key Generation:

It is assumed that name of the sender is Alice and name of received is Bob. Alice wants to sign and send a mesaage M to Bob for verification First Alice selects two random elements p, q € S and a random polynomial f(x) € $Z_{>o}$(X) such that f(p) (≠ 0) € S and then takes f(p) as her private Key, computes y=f(p) ^{m} q, f(p)^{n} and publishes her public key (p.q.y) € S^3

4.5.3 Signature Generation:

Alice performs the following simultaneously and selects randomly another polynomial h(x) € $Z_{>o}$ (x) such that h(p) € S, Then she defines salt as

$u=h(p)^m q\ h(p)^n$ and computes

$r=f(p)^m \{H(M)u\} f(p)^m$ $s=h(p)^m r\ h(p)^n$

$\alpha = h(p)^m\ r\ h(p)^n$ $\beta = f(p)^m\ H(M)\ h(p)^n$

$v_1=h(p)^m\ H(M)h(p)^n$

Then (u,s,α,β, v_1) is the signature of Alice on message M & send it to the Bob for verification and then for acceptance.

4.5.4. Verification:

On receiving the signature (u,s,α,β,v_1) Bob will do the following. For this ,he computes $v_2 = \alpha\ y^{-1}\ \beta$

Bob accepts Alice's signature iff $u^{-1}\ v_1 = s^{-1}\ v_2$, Otherwise, he rejects the signature.

5. DATA TRANSMISSION METHOD USING MULTIPATH ROUTING

5.1 Data Transmission

Let k be number of node disjoint paths from source to destination that were found by suing AODVM, so k≥2 . This section describes the signature transmission through k node disjoint paths. For simplicity here we consider the k=7. Here we use XOR operation between two matrices A and B of size nxm. i.e Let A=[a_{ij}], B = [b_{ij}],C = [c_{ij}] for i=1 to n,for j =1 to m C = A ⊕ B Where $c_{ij} = a_{ij} \oplus b_{ij}$

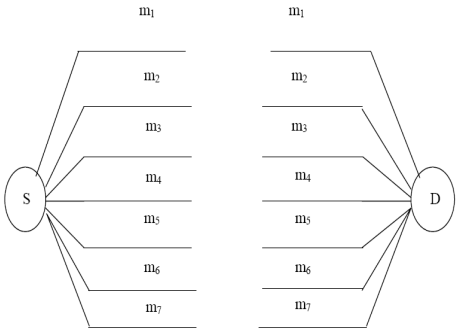
Alice sends (u, s, α, β, v_1) as her signature to Bob, where

$u = \begin{bmatrix} 2 & 16 \\ 10 & 21 \end{bmatrix}$; $s = \begin{bmatrix} 21 & 13 \\ 19 & 07 \end{bmatrix}$; $\alpha = \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix}$;

$\beta = \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix}$; $v_1 = \begin{bmatrix} 5 & 15 \\ 13 & 12 \end{bmatrix}$

The By using signature, Alice generates seven messages m_1, m_2, m_3, m_4, m_5,m_6,m_7 and each message is identified with unique number (ID) and which is sent through a node-disjoint path is shown in fig.1.

Figure .1



Message generation and transmissions

$$m_1 = u \oplus y = \begin{bmatrix} 2 & 4 \\ 10 & 21 \end{bmatrix} \oplus \begin{bmatrix} 4 & 6 \\ 6 & 6 \end{bmatrix} = \begin{bmatrix} 6 & 12 \\ 12 & 19 \end{bmatrix}; \; m_2 = s \oplus u = \begin{bmatrix} 21 & 13 \\ 19 & 7 \end{bmatrix} \oplus \begin{bmatrix} 2 & 16 \\ 10 & 21 \end{bmatrix} = \begin{bmatrix} 23 & 29 \\ 25 & 18 \end{bmatrix}$$

m_2 is sent through path

$$m_3 = \alpha \oplus s = \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix} \oplus \begin{bmatrix} 21 & 13 \\ 19 & 07 \end{bmatrix} = \begin{bmatrix} 29 & 08 \\ 19 & 00 \end{bmatrix}; \qquad m_4 = y = \begin{bmatrix} 04 & 06 \\ 06 & 06 \end{bmatrix};$$

is sent through path 3 and m_4 is public key information and is sent through path 4

$$m_5 = \beta \oplus \alpha = \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix} \oplus \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix} = \begin{bmatrix} 08 & 11 \\ 02 & 11 \end{bmatrix}; \; m_6 = v_1 \oplus \beta = \begin{bmatrix} 5 & 15 \\ 13 & 12 \end{bmatrix} \oplus \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix} = \begin{bmatrix} 05 & 01 \\ 15 & 00 \end{bmatrix}$$

m_5 is sent through path 5 and m_6 is sent through path 6

Through path 7: signal information

m_7 = (4, 7), if k<7 then two or more message are sent through a single node-disjoint paths.

Example if k=3 messages are sent as follows (m_1, m_2), (m_3, m_4),(m_5,m_6, m_7)

5.2 Signature Receiving & Verification:

Bob would not receive the signature from Alice directly. He just receives combinations of parameters of the signature. Using these parameters, Bob calculate exact parameters of signature and then verification will be done for approval.

The procedure as follows:- First Bob received message m_7 from path 7

$m_4 = y = \begin{bmatrix} 04 & 06 \\ 06 & 06 \end{bmatrix}$ is public key information. It was received from path 4

From path 1, message $m_1 = u \oplus y$ was received u is extracted by suing m1 and y as follows:-

$$u \oplus y \oplus y = \begin{bmatrix} 6 & 12 \\ 12 & 19 \end{bmatrix} \oplus \begin{bmatrix} 4 & 6 \\ 6 & 6 \end{bmatrix} = \begin{bmatrix} 2 & 16 \\ 10 & 21 \end{bmatrix} = u; \qquad s \oplus u \oplus u = \begin{bmatrix} 23 & 29 \\ 25 & 18 \end{bmatrix} \oplus \begin{bmatrix} 2 & 16 \\ 10 & 21 \end{bmatrix} = \begin{bmatrix} 21 & 13 \\ 19 & 7 \end{bmatrix} = s$$

From path 2 message $m_2 = s \oplus u$ was received , From path 3 message $m_3 = \alpha \oplus s$ was received, α is extracted by using m_3 and s as follows:-

$$\alpha \oplus s \oplus s = \begin{bmatrix} 29 & 08 \\ 19 & 00 \end{bmatrix} \oplus \begin{bmatrix} 21 & 13 \\ 19 & 07 \end{bmatrix} = \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix} = \alpha \qquad \beta \oplus \alpha \oplus \alpha = \begin{bmatrix} 08 & 11 \\ 02 & 11 \end{bmatrix} \oplus \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix} = \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix} = \beta$$

From path 5 message $m_5 = \beta \oplus \alpha$ was received, β is extracted by using m_5 and α as follows and From path 6 message $m_6 = v_1 \oplus \beta$ was received, v_1 is extracted by using m_6 and β as follows:-

$$v_1 \oplus \beta \oplus \beta = \begin{bmatrix} 05 & 01 \\ 15 & 00 \end{bmatrix} \oplus \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix} = \begin{bmatrix} 5 & 15 \\ 13 & 12 \end{bmatrix} = v_1$$

After receiving the signature of Alice, Bob will do the following for verification i.e he computes

$$V_2 = \alpha y^{-1} \beta = \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix} \begin{bmatrix} 11 & 12 \\ 12 & 15 \end{bmatrix} \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix} = \begin{bmatrix} 20 & 7 \\ 3 & 21 \end{bmatrix}$$

And verifies that

$$U^{-1} V_1 = \begin{bmatrix} 16 & 13 \\ 11 & 07 \end{bmatrix} \begin{bmatrix} 5 & 15 \\ 13 & 12 \end{bmatrix} \bmod 23 = \begin{bmatrix} 19 & 05 \\ 08 & 19 \end{bmatrix};$$

$$S^{-1} V_2 = \begin{bmatrix} 02 & 16 \\ 11 & 06 \end{bmatrix} \begin{bmatrix} 20 & 07 \\ 3 & 21 \end{bmatrix} \bmod 23 = \begin{bmatrix} 19 & 05 \\ 08 & 19 \end{bmatrix}$$

i.e $U^{-1} V_1 = S^{-1} V_2$

Bob accepts alice's signature as a valid signature, otherwise he will reject the same.

CONCLUSION

This paper is mainly concern with authentication and confidentiality during data transmission among the nodes in MANET. We proposed a novel approach for providing the authentication and enhance the data confidentiality. The signature scheme in the transmission designed by using

polynomial symmetrical decomposition problem based on non-commutative division semirigs.The idea is to integrate the signature scheme and multipath routing. Even if an attacker succeeds to have one or lots of transmitted parts, the probability of original message reconstruction is almost negligible.

REFERENCES

[1]. G.S.G.N.Anjaneyulu, P.Vasudeva Reddy, U.M.Reddy " Secured Digital Signature Scheme using polynomials over Non-commutative Division semirings" International journal of computer science and network security, Vol. 8 No.8 pp 278-284
[2]. Souheila Bouam , Jalel Ben – Oathman " Data Security in Ad hoc Networks using multipath Routing" The 14th IEEE International Symposium on personal indoor and Personal Radio Communication Proceedings, **2003**.
[3]. Bing Wu, jianmin chen, Jie Wu, Mihaela Cardei, " A survey on attacks and countermeasures in Mobile Ad Hoc networks", Wireless mobile network security, springer **2006**
[4]. Mahesh.K, Marina and Samir R.das " On-demand multipath distance vector routing in ad Hoc networks ", In proceedings of the 9th international conference on Network Protocols", pp 14-23, November -**2001**
[5]. S.J.Lee and M.gerla " Split Multipath Routing with maximally disjoint paths in Ad Hoc Networks ", In Proceedings of the IEEE, ICC, **2001**, Pages 3201-3205
[6]. L.Wang, Y.shu, Z.Zhao, L.Zhang, and O.Yang " Load Balancing of Multipath source Routing in Ad Hoc Networks", In Proceedings of the IEEE, ICC, **2002**, Vol. 5, Pages 3197-3201
[7]. S.Yi, P.Naldurg and R.Kravets " Security Aware Ad hoc routing for wireless Networks ", Proceedings 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing", long Beach CA, October **2001**, pp.299-302.
[8] K.H. Ko et. al., "New signature scheme using conjugacy problem", Cryptology e print Archive: Report 2002/168, **2002**.
[9] Z. Cao, X. Dong and L. Wang. "New Public Key Cryptosystems using polynomials over Non-commutative rings". Cryptography e-print archive, http://eprint.iacr.org/2007/***
[10] K.H. Ko, *CRYPTO* **2000**. LNCS 1880, PP. 166-183, Springer- verlag, **2000**