Optimization in Architecture of MANET Using Information Retrieval System

Anshu Chauhan, Ashish Aggarwal and Dr. Yaduvir Singh

Abstract— **Wireless links are more vulnerable to attacks they are considered to be "un-trusted" in terms of security, i.e. they are relatively simple to be hacked. Mobile Ad Hoc Networks have unique characteristics like rapid movement of node in infrastructure less network that's changes it's topology, One can easily gain access to confidential information in such case. Also there are problems of generation, distribution and assignment of session key due to a lack of Trusted Model and distributive Certification Authority (CA) for Authentication of mobile nodes in distributed authentication environment. Hence, an Identity-Based secure communication in MANET is discussed in this paper.**

Index Terms— **MANET, Clustering, Threshold cryptography, Lagrange interpolation, ID Based Cryptography.**

I. INTRODUCTION

The use of wireless sensor networks (WSNs) has grown enormously in the last decade, pointing out the crucial need for scalable and energy-efficient routing and data gathering and aggregation protocols in corresponding large-scale environments. A mobile ad hoc network (MANET) [3, 4] is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The mobile nodes connect with each other through radio waves. Due to movement of mobile node the connection dynamically changes during communication.

The main characteristics of MANET are:

- Autonomous Terminal: Each mobile node may function as both a host and a router, usually endpoints and switches are indistinguishable in MANET.

- Distributed Operation: There is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals, each node acts as a relay as needed.

- Dynamically changing topology: Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time.

Communication between mobile nodes in Mobile Ad Hoc networks (MANETs), poses a number of non-trivial clustering and security like problems in distributed authentication environment reacts and faces problems of generation, distribution and assignment of session key due to a lack of Trusted Mode. A passive attack [11] intrudes the data exchange with in the network without varying it. It basically modifies, fabricates, impersonate and replicate the data Attacks in MANET. Distributive Certification Authority (CA) for Authentication of mobile nodes efficiently share authentication information among nodes and Cluster heads (CH) connected by virtual networks.

The exponential increase in the number of nodes in MANET needs proper management hence organizing MANET into different groups, called cluster, each cluster has its own leader Called Cluster head (CH).

A research issue in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between two communicating nodes. The routing protocol must be able to keep up with the high degree of node mobility that often changes the network topology. In a large network, flat routing schemes produce an excessive amount of information that can saturate the network.

In addition, given the nodes heterogeneity, nodes may have highly variable amount of resources, and this produces a hierarchy in their roles inside the network. A distributed certificate authority intended for cluster-based architecture is discussed in this paper. Certificate use for authentication of node and Session key play a important role in secure Communication.

This paper is prepared in sections. Section - I explained about the Introduction. Section - II deals with background that includes related work with reference to present problem and the proposed architecture is discussed in section - III under heads of proposed work the conclusion of this paper is mentioned in section - IV. The proposed work may extended further with reference to different situation are mentioned in section - V under future Aspect, References that's used in this paper.

II. BACKGROUND

Cluster-based routing is a solution to address nodes heterogeneity, and to limit the amount of routing information

Manuscript received February 24, 2015.

Anshu Chauhan, M. Tech Student, Computer Science & Engineering, UPTU, Lucknow (U.P.), India.
Ashish Aggarwal, M. Tech Student, Computer Science & Engineering, MDU, Haryana, India.
Dr. Yaduvir Singh, Associate Professor, Computer Science & Engineering Ideal Institute of Technology, UPTU, Lucknow (U.P.), India.

that propagates inside the network. The idea behind clustering is to group the network nodes into a number of overlapping clusters. Clustering makes possible a hierarchical routing in which paths are recorded between clusters instead of between nodes. The wireless nature and inherit feature of MANET, make it vulnerable to attack. Therefore, the cluster based authentication technique [1] is deployed over of entire MANET.

The main steps can be summarized as:

- The nodes will be divided into clusters with separate cluster head.
- The CH selection and cluster formation procedures should generate the best possible clusters (well balanced, etc.).
- Cluster Head (CH) performs all cluster management operations in cluster.
- Each node have certificate which is issued by certificate authority (CA) for authentication purposes.

There is no central administrative control in MANET, thus Security mechanisms like authentication, data integrity and non repudiation, is deployed by cluster based distributed authentication [2]. A lot of research has been done in the past but none of the protocols have made a decent tradeoff between security and performance. Threshold cryptography key management techniques with Lagrange interpolation [5] is the best way to make the MANET secure. Identity based cryptosystem provides a new but safe strategy for communication in MANET. Identity-based cryptography specifies a cryptosystem in which keys (both public and private) are based on the identities of the users.[3,6]

Transmission based clustering has a disadvantage that the maximum number of nodes in a cluster i.e. threshold number of nodes in a cluster, is not known. Cluster head selection algorithm [7, 8], is used for cluster head election. It also solves the problem of scalability of MANET, CHSA algorithm select only cluster head.

The Highest-Degree Algorithm, also known as connectivity-based algorithm [12]: The degree of a node is computed based on its distance from others. Each node broadcasts its id to the nodes that are within its transmission range. The node with maximum number of neighbors (i.e., maximum degree) is chosen as a clusterhead. The neighbors of a clusterhead become members of that cluster and can no longer participate in the election process. Every time node degree not stable so it not best technique to decide cluster head.

The Lowest-ID, also known as identifier-based clustering algorithm [13]: A unique ID is assigned to each node. A node with the minimum id is chosen as a clusterhead(CH). Thus, the ids of the neighbors of the clusterhead(CH) will be higher than that of the clusterhead(CH). A node is called a gateway if it lies within the transmission range of two or more clusterheads. Whenever a node with a lowest ID is detected in the cluster, the cluster-head must delegate irresponsibility to this node to be cluster-head.so this algorithm is not suitable for MANET.

III. PROPOSED SECURITY ARCHITECTURE AND MECHANISM

In this paper, we propose an information retrieval method on MANET for exchanging information among nodes. It is desirable to satisfy the following four criteria when realizing the information retrieval system on MANET: (1) small power consumption; (2) correct operation even when there is only low communication bandwidth available; (3) small traffic amount; and (4) no concentration of load on particular terminals. This study aims to realize an efficient method which satisfies these criteria.

Architecture for Information Retrieval System:

The proposed architecture is divided in to four modules: Clustering and cluster head election and selection Algorithm, Generate session key using node id and threshold cryptography using Langrange Interpolation, Multi Agent model for secure information retrieval among cluster head.

Clustering and Cluster Head Election and Selection Algorithm: We assign node id to each node by using Random number Generator. After this overall MANET divide into Cluster and each Cluster having own Cluster head (CH). Parameters for Cluster Creation:

MAX Value: Represents the upper bound of the number of nodes that can simultaneously be supported by a cluster-head.

MIN Value: Represents the lower bound of the number of nodes that belong to a given cluster before proceeding to the extension or merging mechanisms.

D Hops Cluster: One hop clusters are too small for large ad hoc networks, therefore SCA creates D hops clusters where D is defined by the underlying protocol or according to the cluster-head state (busy or not).

Identity: Identity (ID) is a unique identifier for each node in the network to avoid any spoofing attacks or perturbation in the election procedure.

Weight: Each node is elected cluster-head (min weight node) according to its weight which is computed from a set of system parameters.

Cluster head plays an important role in Clustering, as there is no central administrative control of MANET so each cluster is managed or control by cluster head. Cluster maintains all the information about the all node reside in the cluster like mobility of node, battery power, Trust value etc. Parameters required for selecting the Cluster Head [14, 15] are:

Belief value (B): Based on previous history of nodes that how much a node is trusted to its neighbor. It's defined as the average of belief values received from each neighboring node.

$$B = \frac{\sum_{i=1}^{N} Bi}{N}$$

Trust value: Defines how much node is trusted to its neighbor. We calculate the average trust value of all node reside in a cluster.

$$T = \frac{\sum_{i=1}^{N} T_i}{N}$$

Degree: Number of neighbors of a given node, within a given radius.

Battery power: Capability of a node to serve as long as possible as cluster head have many responsibility so it must be communicate long time.

Most stable node is elected as a cluster head of cluster. There are following parameter to calculate the stability of node.

Mean distance: Defined as the average of distances between node A and all its neighbors.

$$MD_A = \frac{1}{N}\sum_{n=1}^{N} D_{A,n}$$

Stability: Calculated by using the difference between two value of Mean distance at t and t-1.calculated by this formula

$$ST_A = MD_t - MD_{t-1}$$

Weight Factor: In this we assign weight factor value for each node in cluster in such a way that the summation of all weight factors will be unity.

$$\sum_{i=1}^{n} F_i = 1$$

Global weight: Used to decide the cluster head. Global weight is calculated by using the all above parameter.

W_G [i]= (W_T[i]* F_T[i])+ (W_D[i]*F_D[i])+(W_B[i]*F_B[i])+ (W_M[i]*F_M[i])+ (W_S[i]* F_S[i])

Cluster and cluster Head Creation in MANET

```
I. Assign Node Id for each node of MANET
No of Node = N;
for(i=0; i<N; i++)
  {
    NId[i] =Random NoGenerator( );
  }
/*Random No Generator generate different random Node id for each node in MANET By this way we can provide higher security for secure communication*/
II ClusterCreation( )
{
   TotalNodes=N;
   for(i=0; i<N; i++)
    {
      Each node sends a Beacon Message to its Neighbor to notify its presence to neighbor;
    }
/*Beacon message contains the state of node, each node builds neighbor list based on Beacon Message*/
}
Int Max, Min;
for(i=0; i<N; i++)
{
   if(ClusterNodes< Max)
   {
      joinCluster( );
    }
  if(ClusterNodes>=Max)
    {
      CreateCluster();
    }
 else
    {
        Cluster Merge (); /*if no on node incluster<min_value*/
    }
}
```

```
III Cluster Head Election criteria
ClusterHeadAssignment( )
{
    TotalNodes=n;
    for(i=0; i<n; i++)
     {
      /*Assign Weight for each node in such a way summation of all weight is unity*/

      $W_T$[i]={}; /*Partial Weight factor for trust factor*/
      $W_D$[i]={}; /*Partial Weight factor for node degree*/
      $W_B$[i]={}; /*Partial Weight factor for Battery */
      $W_M$[i]={}; /*Partial Weight factor for Max value*/
      $W_S$[i]={}; /*Partial Weight factor for Stability*/
     /*Take all value from table which is created on the bases of Beacon Message by each node*/
      $F_T$[i]= {}; /* Trust value*/
      $F_D$[i] ={}; /* Node degree*/
      $F_B$[i]={}; /* Battery power*/
      $F_M$[i]={}; /* Max value*/
      $F_S$[i]={}; /* Stability*/
     */calculate Global Weight For each Node*/

$W_G$[i]=($W_T$[i]*$F_T$[i])+$W_D$[i]*$F_D$[i])+($W_B$[i]*$F_B$[i])+($W_M$[i]*
    $F_M$[i])+ ($W_S$[i]* $F_S$[i]);
     }
  Find out minimum Global Weight In Cluster and Assign As Cluster Head (CH);
}
```

```
IV Newly Arriving Node in MANET
i. New node U broadcast Beacon Signal to its neighbor in their transmission Range
ii. Calculate following factor for Newly arriving node FT ,FD ,FB,FM,FS WT,WD, WB, WM and WS calculate WG (Global weight) for newly arrive node.
iii. If(Newly arrive node global Weight <Cluster Head of Cluster)
{
Assign New node as a Cluster head;
}
else
{
JoinCluster();
}
```

V Threshold of battery Power Check the battery power of Cluster Head If(CH_battery Power< PThreshold) CH sends Battery power low Signal to Its Neighbor and recalculate the Global weight for each node and Minimum global weight node assign as Cluster Head else

```
{
    No requirement;
}
```

Generating the Session Key:

To generate session key we will use threshold cryptography and Lagrange interpolation with modular arithmetic, required Minimum t_{Th} (Threshold value) no of node in cluster. Consider a Polynomial equation GF (p) is Finite field p>n Choose a_0, a_1 , a_2 , a_{k-1} $\in$GF (p)

$F(x) = (a_0x^0 + a_1 x^1 + a_2 x^2 + \dots + a_{t-1} x^{t-1}) \bmod p$

F(0)= a0=secret key (SK) and p is a huge prime number and a1, a2…, and ak-1 are arbitrarily chosen from Z/PZ

$$F(x) = \sum_{i=1}^{k} Yi \prod_{1\le j\le k,\, j\ne i} \frac{X - Xj}{Xi - Xj}$$

Lagrange interpolation since f (0) = a_0 = S, the shared secret can be expressed as

$$S = \sum_{i=1}^{k} CiYi \quad \text{Where } C_i = \prod_{1\le j\le t,\, j\ne i} \frac{Xj}{Xj - Xi}$$

Secret key is generated by t arbitrary node (minimum no of threshold node) by using F(0)=$a_0$modp=(SK).

$F(x) = (a_0x^0 + a_1 x^1 + a_2 x^2 + \dots + a_{t-1} x^{t-1}) \bmod p$

```
TotalNodes=N;
for(i=0; i<t; i++)
  {
     NId[i];
  }
for(i=0; i<t; i++)
   {
      nr=1;
     dr=1;
     for(j=0; j<t; j++)
            {
                 If(j≠i)
                   {
                        nr=nr*(x-NId[j]);
                       dr=dr*(NId[i])- NId[j]);
                      F(x)=(nr/dr)*F(NodeId[i]));
 /*Polynomial Equation generated by node id*/
               }
Put the value of x and Generate Secrete KEY;
Sk=F(x) mod p; /*SK-Session Key*/
```

/*This key use as session Key for secure Communication between nodes.*/

Secret Key Generation on the bases of node id using threshold cryptography concept

- Certificate Authority (CA) provides Ceritificate to every node before entering in cluster.
- We will generate Public and private key using RSA algorithm as each node has Public key & Private Key pair issued by CA.
- Cluster Head works as a CA for all nodes in cluster after Receiving Certificate and Key pair from certificate authority (CA).
- CA distributes the session key into t part among Node by using polynomial equation and Node Id.
- To generate session key required Minimum t_{Th} (Threshold value) no of node in cluster ans use above steps.

Multi Agent Model for secure information retrieval among Cluster Heads

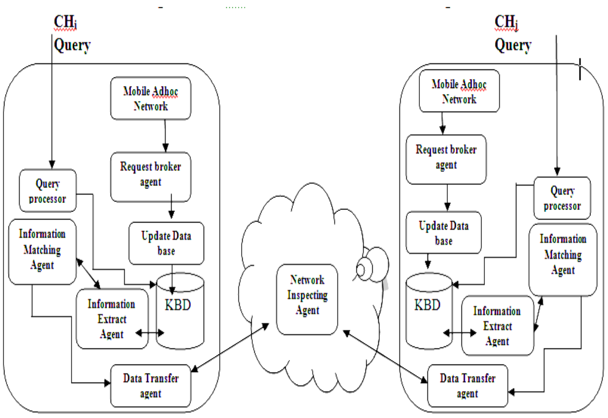

Figure: Multi Agent Model information retrieval among cluster head

Retrieval Broker Agent (RBA): Responsible for managing the cluster's node information such as the identity (MAC address) ,trust value, stability , max value ,battery power ,weight factor , global weight value and retrieval inclinations.

Data Transfer Agent (DTA): DTA is a kind of mobile agent in this architecture. It's responsible for transferring the data and retrieval results among the cluster head.

Information Extract Agent (IEA): It extracts the valuable information from KBD according to query.

Information Matching Agent (IMA): Responsible for receiving information from Information Extract Agent (IEA) and match them and transfer to DTA.

Network Inspecting Agent (NIA): Another kind of mobile agent, traveling among network nodes to investigate the network automatically. NIA is used to detect network error during transferring of data.

Generate Certificate and CLR (Certificate Revocation List) by certificate authority (Certificate X.509)

The traditional approach makes use of X.509 as certificate authority for the nodes participating in the cluster formation. The Secure Hash Algorithm (SHA1) is an efficient algorithm and can also be used for the purpose of providing certificates to nodes thereby providing more security. The SHA (1) algorithm finds its application in the clustering process for making the MANET more reliable and secure.

I propose use of Genetic Algorithm for the purpose of cluster head election. The Weight Factor of the nodes is calculated on the basis of the following three parameters:

a) Energy Dependency
b) Node Velocity as compared to other nodes.
c) Node Density as compared to other nodes.

The Genetic Algorithm with the help of the weight factors of the nodes determines the optimal cluster head

IV. Conclusion

MANET is a type of multi-hop network, infrastructure less and the most important self-organizing. Due to its wireless and distributed nature there is a great challenge for system security designers. Also due to a lack of Trusted Model and distributive Certification Authority (CA) for Authentication of mobile nodes efficiently share authentication information among nodes and Cluster heads (CH) connected by virtual networks. Therefore, We analyzed and optimized a existing threshold cryptography techniques by changing the Certification authority for the purpose of accessing of nodes and using genetic algorithm to calculate the weight factors for computing the optimal cluster head to provide a safe strategy for authentication over Mobile Ad hoc Network. In this paper we have discussed a threshold cryptography technique using Lagrange Interpolation information retrieval system based on Identity-Based in MANET.

V. FUTURE ASPECTS

As the clustering techniques of MANET changed or the heterogeneous nodes with different platform based node interact to each other or retrieving the information from existing one might not be agent's acts appropriately. The proposed architecture and mechanism will provide efficient and effective security to nodes in MANET but as number of nodes over network is scaled up beyond certain limit them performance might be reduced.

VI. REFERENCES

[1] R. Murugun, S. Shanmugam ―Cluster based authentication techniques for mitigation of internal attacks in MANET‖. ISSN 1450-216X VOL-51 No-3 (2011) PP.433-441.

[2] Nevadita Chateerjee,Anupama Potluri and Atul negi, "Self organizing approach to MANET Clustering.

[3] Shushan Zhao, Akshai Aggarwal , Richard Frost, Xiaole Bai , A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks , IEEE communications surveys & tutorials, vol. 14, No. 2, Second Quarter 2012.

[4] Lu Li, Ze Wang, Wenju Liu and Yunlong , A Certificate less Key Management Scheme in Mobile Ad Hoc Networks , 2011 IEEE.

[5] Li Wang, Jiu Hui Zhang ― Security Strategy of MANET Based on Identity- Based Cryptosystems‖ 978-1-4244-5143-2/10/$26.00 ©2010 IEEE.

[6] Eduardo Da Silva , Aldri L. Dos Santos, Andluiz Carlos P. Albini , Identity based key management in mobile adhoc networks and applications, IEEE Wireless Communications, October 2008.

[7] Dang Nguyen1, Pascale Minet2, Thomas Kunz3 and Louise Lamont1 ―On the Selection of Cluster Heads in MANETs‖ Communications Research Centre Ottawa, ON K2H 8S2, Canada INRIA Rocquencourt Rocquencourt, Le Chesney Cedex 78153, France 3 Dept. of Systems and Computer Engineering, Carleton UniversityOttawa, ON K1S 5B6, Canada IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814.

[8] Kadri†, A. M'hamed††, M. Feham ―Secured Clustering Algorithm for Mobile Ad Hoc Networks‖ National Institute of Telecommunications, Evry, France IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007.

[9] Pradeep Rai Asst. Prof., CSE Department, Asst. Shubha Singh Prof., MCA Department, ―A Review of ‗MANET's Security Aspects and Challenges‖ IJCA Special Issue on ―Mobile Ad-hoc Networks‖MANETs, 2010.

[10] XU Xiao-long XIONG Jing-Yi, CHENG Chun-Ling ―The Model and the Security Mechanism of the Information Retrieval System based on Mobile Multi- Agent‖ 978-1-4244-6871-3/10/$26.00 ©2010 IEEE.

[11] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, ―A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks‖, Wireless Network Security, Springer Book, ISBN: 978-0-387- 28040-0, pp. 103--135, 2007.

[12] M. Gerla and J.T.C. Tsai. Multicluster, ―mobile, multimedia radio network, Wireless Networks‖. Vol. 1, No. 3, 1995, PP. 255–265.

[13] H. Luo and S. Lu, ―Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks‖. Technical Report 200030, UCLA Computer ScienceDepartment 2000.

[14] M. Chatterjee, S. K. Das and D. Turgut. *WCA: "*A WeightedClustering Algorithm for Mobile Ad hoc Network"s. Journal of Cluster Computing (Special Issue on Mobile Ad hocNetworks), Vol. 5, No. 2, April 2002, pp. 193-204.].

[15]. I.I. ER, and Winston K. G. Seah, "Mobility-based D-hop Clustering Algorithm for Mobile Ad hoc Networks". IEEE WCNC, Atlanta, USA, March 2004.

[16] D.J. Baker and A. Ephremides. "The Architectural Organization of a Mobile Radio Network Via a Distributed Algorithm", IEEE Transactions on Communications(PP. 1694–1701), COM- 29- 11 (1996).

[17] Basagni S., "Distributed Clustering for Ad Hoc Networks", Proceedings of International Symposium on Parallel Architectures, Algorithms and Networks, (PP. 310- 315), Jun. 1999.