International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-2, July 2013

Secure Communication Architecture Based On "BBCMS" Clustering Algorithm for Mobile Adhoc Network (MANET)

Heenavarshney, Pradeep Kumar

Abstract- Mobile ad hoc networks are self created and self organized without the support of network infrastructure, consists of mobile devices, such as laptops, cell phones, etc. Security is one of the prime Issues in ad hoc network due to their rapidly change in topology and mobility of nodes. However, the infrastructure less and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. We propose a Secure Communication architecture based on "BBCMS" clustering algorithm. In this algorithm elect cluster head (CH) according to its weight computed by combining a set of system parameters (Stability, Battery, connectivity … etc). It also overcomes some limits in Existed algorithms by defining new mechanisms as cluster dissection, assimilation. In the proposed architecture, the overall network is divided into clusters where the cluster-heads (CH) are connected by virtual networks. For secure data transmission, credential authority (CA) issues a certificate (X.509) to the requested node for authentication. The certificate of a node is renewed or rejected by CH, based on its trust counter value.

Keywords–BBCMS, CertificateX.509, CA, Mobile Ad-Hoc Networks,

I. INTRODUCTION

MANETs are autonomous systems consisting of mobile hosts that are connected by multi-hop wireless links. MANETs are decentralized networks that develop through self organization. In mobile ad hoc network there is no fixed infrastructure therefore the mobile hosts communicate over multi-hop wireless link. MANETs have the following inherent Characteristics: open medium, lack of fixed central structure, dynamically changing topology, constrained capability, less bandwidth, rely on batteries, etc, So MANETs are highly vulnerable to various security attacks.

Providing secure Communication in MANET proved to be significant challenge. Authentication and Trust Model which are developed for wired network cannot be used in wireless network. Common authentication schemes are not applicable in Ad hoc network since public key infrastructure is hard to deploy.

Security Threats on MANET

The security threats confronted by MANET is the extension and expansion of that be confronted by wired Network in the wireless field, which mainly comes from wireless channels and networks. The threats can be Divided into two categories of passive attack and active attack.

Manuscript published on 30 July 2013.
*****Correspondence Author(s)
Heena Varshney, Computer Science & Engineering, MTU, Noida (U.P), India.
Pradeep Kumar, Computer Science & Engineering, Shobhit University, Jss Academy of Technical Education, Noida (U.P), India.

A. Passive Attack

Passive attack is essentially to listen or surveillance the message transmission process to obtain some secret, which mainly includes two kinds of wiretapping and traffic analysis. Wiretapping is to intercept packets being transmitted and access to confidential information. Traffic analysis is to analyze characteristics of packet frequency, length and etc to hypothesize the content of communication.

B. Active Attack

Active attack will tamper data stream. The active attack includes four kinds of message replay, fraud counterfeiting, message tampering and denial of service.

As security point of view Clustering play important role in MANET. A way to support the increasing number of nodes in MANET is to subdivide the whole network into groups, and then create a virtual backbone between delegate nodes in each group. In ad hoc network this operation is called clustering, giving the network a hierarchical organization. Among all security issues in MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure to secure applications and network services Certification is a prerequisite to secure network communications. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer, and can be used to verify that a public key belongs to an individual and to prevent tampering and forging in mobile ad hoc networks. Certificate revocation is an important task of enlisting and removing the certificates of nodes that have been detected to launch attacks on the neighborhood. In other words, if a node is compromised or misbehaved, it should be removed from the network and cut off from all its activities immediately. Certificate use for authentication of node and Session key play a important role in secure Communication. This paper is organized in sections. Section - I explained about Introduction. In section - II deals with background that includes related work with reference to present problem moreover the proposed architecture is discussed in section - III under heads of proposed work, the architecture of this paper is mentioned in section - IV. The proposed work conclusion is mentioned in section – V, future Aspect is mentioned in Section VI, References included in section – VII that's used in this paper.

II. BACKGROUND

A. Highest-Degree Algorithm

The Highest-Degree Algorithm, also known as connectivity-based algorithm was originally proposed by Gerla and al.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

This algorithm is based on the degree of nodes assumed to be the number of neighbors of a given node. Whenever the election procedure is needed, nodes broadcast their Identifier (ID) which is assumed to be unique in the same network. According to the number of received IDs every node computes its degree and the one having the maximum degree becomes cluster-head. Major drawbacks of this algorithm are the number of nodes in a cluster is increased, the throughput drops and hence a gradual degradation in the system performance is observed.

B. Lowest-ID Algorithm

The Lowest-ID, also known as identifier-based clustering algorithm, was originally proposed by Baker and Ephremides. This algorithm assigns a unique ID to each node and chooses the node with the minimum ID as a cluster-head. Whenever a node with a lowest ID is detected in the cluster the cluster-head must delegate it responsibility to this node to be cluster-head. Major drawbacks of this algorithm are its bias towards nodes with smaller ids which may lead to the battery drainage of certain nodes, and it does not attempt to balance the load uniformly across all the nodes.

C. Mobility-Based d-Hop Algorithm

This algorithm proposes a clustering scheme based on the real distance between nodes. Proposed to calculate an estimate value of the distance between nodes by measuring the received signal strength taken from periodic beaconing or hello messages used in some routing protocols. According to this estimated value they can determine the stability of every node. Then they elect the most stable node as cluster-head

D. Weighted Clustering Algorithm WCA

The Weighted Clustering Algorithm (WCA) was originally proposed by M. Chatterjee et al. It takes four factors into consideration and makes the selection of cluster-head and maintenance of cluster more reasonable. The four factors are node degree, distance, mobility and remaining battery power respectively. And their corresponding weights are w1 to w4. Although WCA has proved better performance than all the previous algorithms, it lacks a drawback in knowing the weights of all the nodes before starting the clustering process and in draining the CHs rapidly. As a result, the overhead induced by WCA is very high.

E. Secured Clustering Algorithm for Mobile Ad Hoc Networks

This algorithm is a secured weight-based clustering algorithm allowing more effectiveness, protection and trust in the management of cluster size variation. It includes security requirements by using a trust value defining how much any node is trusted by its neighbor hood, and using the certificate as node's identifier to avoid any possible attacks (Spoofing). SCA elects cluster-head according to its weight computed by combining a set of system parameters (Stability, Battery, Degree … etc).

III. PROPOSED SECURITY ARCHITECTURE

The proposed architecture is divided in number of modules like Clustering and cluster head election criteria and the X.509 certificate which we are using for authentication of node.

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).
There is different no of parameter for clustering
MAX VALUE, MIN VALUE, D HOPE, IDENTITY, WEIGHT

A. Cluster Head election criteria

Cluster head play is important role in Clustering, because there is no central administrative control of MANET so each cluster is managed or control by cluster head .Cluster maintain all the information about the all node reside in the cluster like mobility of node, battery power ,Trust value etc. Following Parameter are used to elect the cluster head of Cluster.

- **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.

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

- **Connectivity (C):** Is the number of neighbors of a given node, within a 2d hop.
- **Battery power (b):** Power play a important role to decide the cluster head because cluster head have many responsibility so it must be communicate long time.
- **Max Value (M):** Defines a number of nodes that a cluster head (CH) can handle within the cluster.
- **Stability (S):** It is also useful parameter to decide the cluster head. Most stable node elect as a cluster head of cluster. There are following parameter to calculate the stability of node.
- **Distance:** the distance between two nodes A, B is the number of hops between them

$$D_{A,B} = = \sum\sqrt{((x_2 - x_1)^2 + (y_2 - y_1))^2}$$

- **Average distance:** defined as the average of distances between node A and all its neighbors

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

N is the degree of A. when *AD* = 2 this means that the majority of neighbors are within 2 hops

- **Mobility:** Calculated by using the difference between two value of Average distance at t and t-1.

$$MTA = AD_t - AD_{t-1}$$

- **Weight Factor:** Weight factor also play a very important role to decide the cluster head. Weights are assigned to nodes such that their summation is unity.

$$\sum_{i=1}^{N} W_i = 1$$

B. Global weight

This is the main parameter to decide the cluster head. Global weight is calculated by using the all above parameter. Node that has the minimum value will elect as a cluster head.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

$$W_G[i] = (W_B[i] * F_B[i]) + (W_C[i] * F_C[i]) + (W_b[i] * F_b[i]) + (W_N[i] * F_N[i]) + (W_S[i] * F_S[i])$$

C. Working Operation

Firstly every node gets the certificate from the Certificate authority. Random no generator assign the node id to each node. After assigning node id MANET is divided into Cluster by using transmission range based cluster like (2 hop).

Each cluster has one important node assign as a Cluster Head, Cluster head is decided on the basis of different parameter by using Cluster head election module, Review module use to reassign of cluster head if the power of presently cluster head is less than the threshold power.

Session key generated by using node id, Key use as a session key for secure communication.

PHASE-1: Cluster and cluster Head Creation in MANET

Step-I. Assign Node Id for each node of MANET

No of Node = N;
For (i=0; i<N; i++)
{
Node Id[i]=Random No Generator( );
}
/*Random No Generator generate different random Node id for each node in MANET By this way we can provide higher security for secure communication*/

Step-II Cluster Creation ( )

{ Total No of Node=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 Value, Min Value;
for(i=0; i<n; i++)
{
if(No of node in Cluster< Max_value)
{
join cluster( );
}
if(No of node in Cluster>=Max_value)
{
Create new cluster();
}
else
{
Cluster Assimilation ()/*if no.of nodes in cluster <min. value*/
}
}

STEP-III Cluster Head Election criteria
Cluster Head Assignment ( )

{
Total No of Node=n;
for(i=0; i<n; i++)
{
/*Assign Weight for each node in such a way summation of all weight is unity*/
W_B [i]={}; /*Partial Weight factor for belief value*/
W_C[i]={};/*Partial Weight factor for node connectivity*/
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_B[i]= {}; /* Belief value*/
F_C[i]={}; /* Connectivity*/
F_b[i]={}; /* Battery power*/
F_M[i]={}; /* Max value*/
F_S[i]={}; /* Stability*/
/calculate Global Weight For each Node/
} Find out minimum Global Weight In Cluster and Assign as Cluster Head (CH);
}

STEP-IV Newly Arriving Node in MANET

A. New node U broadcast Beacon Signal to its neighbor in their transmission Range
B. Calculate following factor for Newly arriving node F_B ,F_C, F_b, F_M, F_S ,W_B, W_C, W_b, W_M and W_S calculate WG (Global weight) for newly arrive node.
C. If(Newly arrive node global Weight <Cluster Head of Cluster)
{
Assign New node as a Cluster head;
}
else
{
Join Cluster();
}

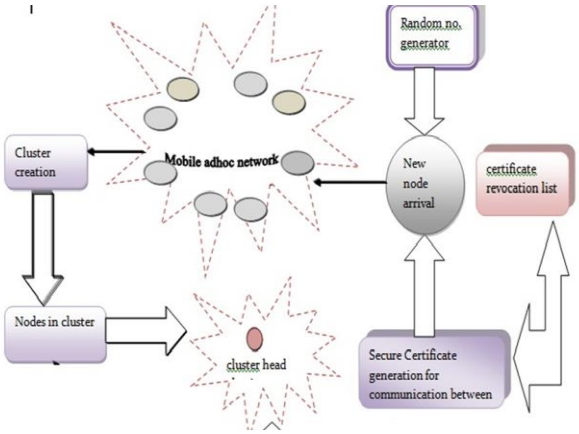
STEP-V Threshold of battery Power

Check the battery power of Cluster Head
If(CH_battery Power< Threshold)
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;
}

STEP-VI Generate Certificate and CLR (Certificate Revocation List) by credential authority (Certificate X.509)

In this phase we are using here X.509 Certificate to authentication of MANET node and new arrival node

IV. PROPOSED ARCHITECTURE



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

V. CONCLUSION

Security has become a prime concern for providing security while communication between mobile nodes in Mobile Ad Hoc networks (MANETs), due to its unique characteristics like rapid movement of node in infrastructure less network that's changes it's topology. By using X.509 certificates and certificate revocation list we can provide a good security to the network.

Including the security features through the use of BEACON mechanism to elect the most trusted node, we've also proposed to use certificate as identifier to avoid spoofing attacks. Defining a set of system parameters for the election procedure to elect the most power node as cluster-head, as well as a new method to compute stability more simple and possible to be used in ad hoc network also defining an upper and lower bounds to limit the number of nodes in clusters.

VI. FUTURE ASPECTS

The proposed architecture will provide efficient and effective security to nodes in MANET and can be applied to heterogeneous network. But as number of nodes over network is scaled up beyond certain limit them performance might be reduced

REFERENCES

1. Ratish Agarwal, Dr. Mahesh Motwani, "Survey of clustering algorithms for MANET". International Journal on Computer Science and Engineering Vol.1 (2), 2009,98-104
2. Mohammad Shayesteh and Nima Karimi, Member, IACSIT," An Innovative Clustering Algorithm for MANETs Based on Cluster Stability", International Journal of Modeling and Optimization, Vol. 2, No. 3, June 2012
3. Yao Yu+, Lincong Zhang "A Secure Clustering Algorithm in Mobile Ad Hoc Networks" IPCSIT vol. 29 (2012).
4. Salaheddin Dervish, Simon J. E. Taylor and Gheorghita Ghinea "Security Server-Based Architecture for Mobile Adhoc Networks" 2012 IEEE 11th International Conference
5. B. Kadri, A. M'hamed, M. Feham "Secured Clustering Algorithm for Mobile Ad Hoc Networks" IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007
6. Nevadita Chatterjee, Anupama Potluri and Atul negi, **"**Self organizing approach to MANET Clustering".
7. Atef Z. Ghalwash, Aliaa A. A. Youssif, Sherif M. Hashad and †Robin Doss "Self Adjusted Security Architecture for Mobile Ad Hoc Networks" 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007).
8. R. Murugan, A. Shanmugam," A Cluster Based Authentication Technique for Mitigation of Internal Attacks in MANET" ISSN 1450-216X Vol.51 No.3 (2011), pp.433-441.
9. Chatterjee, M., Das, S., & Turgut, D. "WCA: A Weighted Clustering Algorithm (WCA) for mobile ad hoc networks". Cluster Computing (PP. 193- 204). Kluwer Academic, 2002.
10. Abdel Rahman H. Hussein, Sufian Yousef, and Omar Arabiyat "A Load-Balancing and Weighted Clustering Algorithm in Mobile Ad-Hoc Network"
11. R.PushpaLakshmi "Cluster Based Composite Key Management in MobileAd Hoc Networks" International Journal of Computer Applications Volume 4 – No.7, July 2010.
12. *S.*Muthuramalingam and *R.Rajaram"* A TRANSMISSION RANGE BASED CLUSTERING ALGORITHMFOR TOPOLOGY CONTROL MANET*"* International journal on applications of graph theory in wireless ad hoc networks and sensor networks Vol.2, No.3,Septembe r 2010

AUTHOR PROFILE

Heena Varshney is pursuing M.Tech (Computer Science & Engineering) from Jss Academy of Technical Education Noida (U.P), Mahamaya Technical University and B.Tech (Computer Science) from Mahatma Gandhi Mission College of Engineering & Technology Noida (U.P), Gautam Budhh Technical University.

Pradeep Kumar is working as Assistant Professor in JSS Academy of Technical Education Noida (U.P). He has worked as a Assistant Professor in Mahatma Gandhi Mission College of Engineering & Technology Noida (U.P.). He has completed his M-Tech (Computer Engineering) from Shobhit University. B-Tech (Computer Science) from College of Engg. Roorkee, Uttarakhand (U.K). During his teaching he has coordinated several Technical fests. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national and international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security