An effective cluster formation with security in mobile ad hoc network

P.Buvana*
Assistant Professor department of CSE
K.S.Rangasamy college of technology,tiruchengode
Namakkal, India
pbuvanacse@gmail.com

S.Geetha**
PG scholar department of CSE
K.S.Rangasamy college of technology,tiruchengode
Namakkal, India
gheethacse@gmail.com

ABSTRACT

Mobile ad hoc networks have attracted much attention due to their mobility and easy deployment. However, the wireless and dynamic nature of network renders them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services. The Clustering Problem in MANETs consists of selecting the most suitable nodes of MANET topology as clusterheads, and ensuring that regular nodes are connected to clusterheads such that the lifetime of the network is maximized. In this paper, Enhanced balanced clustering algorithm with distributed self-organization (EDSBCA) is proposed for cluster formation. Elliptic Curve Digital Signature algorithm (EC-DSA) based authentication scheme is implemented in clustering of MANET for securing the nodes in cluster. Extensive results demonstrate that the scheme is effective and efficient to guarantee security in mobile ad hoc networks.

Keywords: cluster, ECDSA, EDSBCA, authentication, ECC, multi-hop,

1.INTRODUCTION

Mobile ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility nature, dynamic topology, and ease of deployment. A mobile ad hoc network is a self-organized wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. In addition to mobility[2], mobile devices cooperate and forward packets with each other to extend the limited wireless transmission range of each node by multi-hop relaying, which is used for various applications e.g., disaster relief, military operation, and emergency communications [15]. Network is divided into clusters and EDSBCA algorithm is used for cluster formation.

Security is one crucial requirement for these network services [1]. Hence cryptography algorithm is used here for security. The wireless and dynamic natures of MANET expose them more vulnerable to various types of security attacks than the wired networks. It is difficult to secure mobile ad hoc networks, because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Another issue that has a major impact on the performance of a routing protocol is scalability [4]. Scalability is defined as the ability of a network to adjust and maintain its performance when the number of member nodes increases. In clustering the mobile nodes in a MANET are divided into different virtual groups, and they are allocated geographically adjacent into the same cluster according to some rules based on the algorithm with different behaviors for nodes included in a cluster [9]. A clusterhead normally serves as a local coordinator for its cluster, performing intra-cluster transmission, data forwarding and so on. A cluster gateway is a non-clusterhead node with inter-cluster links, so it can access neighboring clusters and forward information between clusters. A cluster member is usually an ordinary node.

Elliptic curve cryptography (ECC) has ability to provide equivalent security as RSA but at much smaller key sizes and at fast rates [13]. The ECC based DSS is also called as Elliptic Curve Cryptography Digital Signature algorithm (ECDSA). It defines two important procedures for digital signature generation and verification based on domain parameters. This provides Authentication, Integrity and non reputation. ECC [11] has been considered for applications such as smart card encryption due to less storage requirements and fast rates. ECDSA consists of signature generation and signature verification phase.

2.RELATED WORK

Cluster formation algorithm, DS-based clustering is based on routing a set of dominating nodes, which function as the clusterheads to relay routing information and data packets, is a technique in MANETs[5]. A DS is called a connected DS (CDS) if all the dominating nodes are directly connected with each other. Chen's Wu

CDS Algorithm is distributed algorithm to find a CDS in order to design efficient routing schemes for a MANET. The objective of the two DS-based clustering schemes is to attempt to select a small number of mobile nodes as dominating. Both schemes form 1-hop clusters with dominating nodes serving as clusterheads. Compared with Wu's algorithm, Chen's algorithm can form fewer clusters, resulting in less overlapping cluster architecture by reducing the direct connection requirement between dominating nodes.

Low-maintenance clustering algorithm[8] is used to reduce the communication overhead caused by cluster maintenance. Low-maintenance clustering protocols usually aim at providing stable cluster architecture by reducing the re-affiliation rate and especially minimizes re-clustering situations. It eliminates the control overhead for clustering completely by constructing and maintaining cluster architecture based on data traffic forwarding.

LCC (Least Cluster Change) is considered to be a significant enhancement of Lowest ID Clustering. In LCC the clustering algorithm is divided into two steps: cluster formation and cluster maintenance. LCC significantly improves cluster stability but large communication overhead occurs. 3hBAC (3-hop Between Adjacent Clusterheads)[8] a non-overlapping cluster structure can be achieved with the introduction of cluster guest. This can reduce the number of clusters and eliminate small unnecessary clusters like LCC.

In Lin's Algorithm [8] every mobile node keeps its own ID and ID of its direct neighbors. Each mobile node that declares to be a clusterhead set its own ID as its cluster ID (CID). Initially, mobile nodes with the lowest IDs become cluster-heads. PC (Passive Clustering) is a clustering protocol that does not use dedicated clustering-protocol specific control packets or signals, so it is called Passive Clustering[14]. In PC, a node can be in one of the following four states: initial, clusterhead, gateway, and ordinary node.

Weight-based distributed Clustering Algorithm (WCA)[5] can dynamically adapt itself with the ever changing topology of the network. This algorithm takes into consideration the degree, transmission power, mobility, and battery power of mobile nodes. WCA, can improve system performance, maintain network security, and have good generality. PCA algorithm adopts distance, relative speed and degree difference as metrics and selects proper CH and maintain cluster. Here energy consumption is not considered.

The DSBCA algorithm is based on the connectivity density and the distance which is applied in wireless sensor network[7].

In security aspect nodes must be secured from attackers[6]. Hence various security schemes are adopted. If data is secured and then node gets hacked by attacker then there is no use of security. Password authentication scheme in public key cryptography (PKC) is adopted for authentication in existing work[10]. Signature is generated to authenticate with nodes.

3. PROPOSED SYSTEM

EDSBCA algorithm is adopted for effective cluster formation by electing suitable cluster head nodes. Security for the nodes in cluster is provided by ECC based algorithm ECDSA.

3.1 Cluster formation

Cluster Head election is the key to cluster stability and this significantly improves network performance. Our Enhanced balanced clustering algorithm with distributed self-organization (EDSBCA) modifies the DSBCA to elect suitable CHs and partition the network into clusters. Specifically, our EDSBCA adopts distance, density, energy and velocity as metrics to periodically select proper CHs in a distributed manner[7], and nodes besides CHs select one CH to join, forming logically non-overlapped multi-hop clusters. Particular threshold value is set to medium for all parameters. When this condition is satisfied by any node then higher value node is chosen for electing CH. First, the nodes estimate the density with that higher density nodes become cluster-head. After the estimation, if both nodes have same density then distance is measured with member nodes minimum distance node here become cluster-head. Finally, distances are same then energy is considered and if energy is same then velocity is considered but only if the condition is satisfied. EDSBCA can be divided into three stages: cluster-head selecting phase, clusters building phase and cycle phase.

Cluster Head Selecting Phase

EDSBCA selects the random nodes to trigger clustering process first. Then the trigger node calculates its connected nodes density becomes the temporary cluster head. EDSBCA follows a distributed approach to build hierarchical structure in self-organizing mode without central control.

$D_k=(|(t,v) \in E/t,v \in N_k(u) U\{u\}|) / (| N_k(u)|)$

In this phase, nodes density, distance, energy and velocity are calculated then the nodes satisfying the condition are all selected with those nodes highest degree node is elected as cluster head. In the initial stage, the node U_t triggers the clustering process and sends Hello messages to its k-hop neighbors. If both nodes have same density then distance is measured with member nodes minimum distance node here become CH. Finally, if distances are also same then energy is considered higher energy node become CH. If energy is same then velocity is considered.

When CH is elected then cluster head node broadcasts Head_message to its k-hop neighbors to declare itself as cluster head and asks them to join the cluster. Head_message includes the ID of cluster head node (HID), the ID of the sending node (SID) and the number of hops from the cluster head. In EDSBCA algorithm, if the node does not receive Head_message in waiting time T(w). (T(w) < T(k)), it declares itself the cluster head, where T(w) is waiting time, and T(k) is the refresh time related to distribution of nodes. The settings of T(w) and T(k) should ensure that each node in the network can find its own cluster head, and the algorithm restarts the clustering process after T(k) circularly. Figure 3.1 shows clustering distribution in this algorithm.

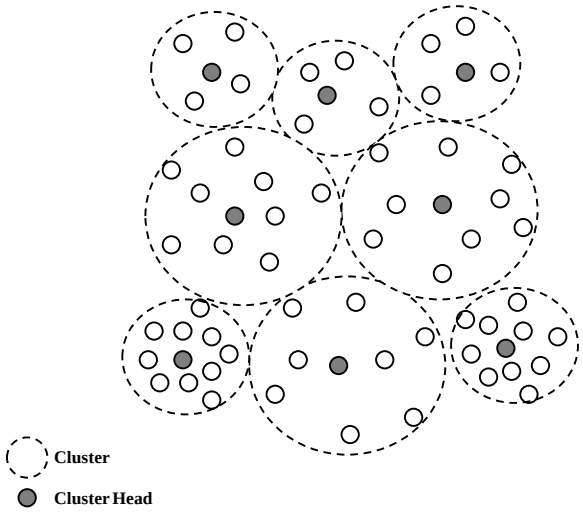

Figure 3.1 EDSBCA Clustering

Clusters Building Phase

EDSBCA sets the threshold of cluster size. The number of cluster nodes cannot exceed the threshold to avoid forming large clusters, which will reduce extra overhead and thus reduce network lifetime. When the cluster head node receives Join_message sent by the ordinary node, it will compare the size of cluster with threshold to accept new member and update the count of cluster nodes if the size is smaller than threshold, or reject the request.

Each member node of cluster maintains a cluster information table, which saves the HID, HD, SID and other information. If a node receives transmitting packet in work, it will update its cluster information table correspondingly. EDSBCA algorithm avoids the fixed cluster head scheme with periodic replacement to balance the node energy consumption.

Cycle Phase

The cluster is stable for a while until the process of reelecting cluster head is triggered in T(k). The cluster head gathers the weight of all member nodes, and then selects the node with highest weight as the next head node. The reelecting of cluster head occurs in the old cluster, so the broadcast of temporary head and the corresponding responses of all the k-hops neighbors are unnecessary. Here communication cost is reduced and the cycle continues. EDSBCA can form more reasonable cluster structure to avoid frequent exchange of the nodes information and temporary cluster head broadcasting after the first clustering. As a result, the energy consumption decreases effectively. EDSBCA maintains effectively stable clustering structure in which switching of cluster head often occurs in the same cluster.

3.2 Security

Elliptic Curve Digital Signature Algorithm (ECDSA) based authentication scheme

Elliptic curve cryptography, the bit size of the public key needed for ECDSA is twice the size of the security level[12], in bits. By comparison, at a security level of 80 bits, for example an attacker requires the equivalent of about 2^{80} signature generations to find the private key, the size of a DSA public key is at least 1024 bits, whereas the size of an ECDSA public key would be 160 bits which is better. The ECDSA[3] is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups, ECC. In order to involve in secure and trusted communication, both parties must concur upon Elliptic Curve domain parameters. It includes two steps.

Signature generation

Nodes want to communicate with the cluster send request to CH, it verifies the node and send a signature to requested node which consists of CH id, request node id and time of expiry which is encrypted in private key known only by CH. By using that it can communicate with the cluster member nodes.

Signature verification

When the member node receives the signature it decrypts it with the public key and verifies the CH and sending node id and time then it accepts communication. Hence ECDSA is adopted for signature generation and verification. This scheme is effective here in authentication, integrity and confidentiality.

4. CONCLUSION

Clustering provides better performance of the protocols by improving throughput, scalability, power consumption and reduces redundancy. Due to the mobility and dynamic nature, the mobile ad hoc networks are much more prone to various kind of security risks, such as information disclosure, intrusion, or even denial of service attacks. Maintenance of MANET is easier with clustering. Cluster-based MANET has many important issues to examine, such as the cluster structure stability, the control overhead of cluster construction and maintenance, the energy consumption of mobile nodes, the load distribution in clusters and also security is a major problem.

Clustering algorithms Wu's CDS algorithm, Chen's WCDS algorithm, LCC, 3hBAC, Lin's algorithm require the assumption of frozen period of motion for mobile nodes. PC does not depend on this stationary assumption because it is based on a "first claim wins" solution for the initial cluster formation. WCA causes computing and communication overhead in maintaining nodes weight.

Our proposed EDSBCA algorithm for cluster formation elects suitable CHs and maintain cluster effectively. It reduces communication cost, improves the network life cycle significantly. The ECC offers more security per bit than any other standardized public key cryptography scheme. Smaller key size, high performance, lower computational cost, and a relatively fast signature generation can be achieved through ECDSA. Wireless devices are rapidly becoming more dependent on security features such as the ability to secure email, secure Web browsing, and virtual private networking to corporate networks, where ECC allows more efficient implementation of all of these features.

5. REFERENCES

[1] Ahmad Khadem-Zadeh, Jamshid Bagherzadeh, Mohammad Masdari, Mohammad Reza Ahmadi and Sam Jabbehdari(2011), "A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks", EURASIP Journal on Wireless Communications and Networking,Vol.2,No.1,pp.80-91.

[2] Assim Sagahyroon, Fadi Aloul, Syed Zohaib Hussain Zahidi and Wassim El-Hajj (2013) "Optimizing Complex Cluster Formation in MANETs Using SAT/ILP Techniques", IEEE sensors journal, Vol.13, No.6, pp.2400–2412.

[3] Asvhini Subramaniam, Junaid Ahsenali Chaudhry, and Mudassar Ahmad(2012), "A Study on Elliptic Curve Digital Signature Algorithm (ECDSA) for Reliable E-Commerce Applications" Smart Computing Review, Vol. 2, No. 1,pp.71-78.

[4] Diana Tabet, Haidar Safa, Hassan Artail(2009), "A cluster-based trust-aware routing protocol for mobile ad hoc networks",Vol.11,No.4,pp.969–984.

[5] Guann-Long Chiou , I-Ta Lee, Shun-Ren Yang (2011), "A cooperative multicast routing protocol for mobile ad hoc networks", Vol.11, No.4, pp.2407–2424.

[6] Hiroki Nishiyama, Jie Yang, Nei Kato, Nirwan Ansari and Wei Liu (2013), "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions On Parallel And Distributed Systems,Vol. 24, No. 2,pp. 239-249.

[7] Huan Qi, Weiqun Li and Ying Liao (2013), "Load-Balanced Clustering Algorithm With Distributed Self-Organization for Wireless Sensor Networks", IEEE sensors journal, Vol. 13, No. 5, pp. 1498-1506.

[8] Jane y. Yu and peter h. J. Chong (2009) "A Survey of clustering schemes for Mobile ad hoc networks", IEEE Communications, Vol.7, No.1, pp.969–986.

[9] Jiannong Cao , Michel Raynal and Weigang Wu (2009) "Eventual Clusterer: A Modular Approach to Designing Hierarchical Consensus Protocols in MANETs", IEEE transactions on parallel and distributed systems, Vol.20, No.6, pp.753–765.

[10] Jie Li, Mohsen Guizani and Yongsheng Liu (2012), "PKC Based Broadcast Authentication using Signature Amortization for WSNs" IEEE transactions on wireless communications, Vol. 11, No. 6, pp. 2106-2115.

[11] Kristin lauter (2004), "The advantages of Elliptic curve cryptography for Wireless security",IEEE Wireless Communications Vol.21, No.5,pp. 1536-1284.

[12] Ms. B. Lavanya, Dr. (Mrs). G.Padmavathi (2012), "Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for Small Mobile Adhoc Networks" Int. J. Advanced Networking and Applications, Vol.03, No.04, Pages.1245-1252.

[13] Levent Ertaul, Nitu Chavan (2005), "Security of Ad Hoc Networks and Threshold Cryptography" IEEE Vol.08, No.02, pp.9303-9309.

[14] Peng Zhao, Xinyu Yang, Wei Yu, and Xinwen Fu (2013) "A Loose-Virtual-Clustering-Based Routing for Power Heterogeneous MANETs" IEEE transactions on vehicular technology, Vol.62,No.5,pp.2290–2302.

[15] A. Scaglione, D. Goeckel, J. Laneman (2006), "Cooperative communications in mobile ad hoc networks", IEEE Signal Processing Magazine Vol.10,No.3, pp18–29.