Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 1 (2015), pp. 165-176

http://www.ripublication.com

Fault Tolerant Group Key Management Inter Clustering Approach

[1]Meera Gandhi.G, [2]Christy.A
[1]Professor, Faculty of Computing, Sathyabama University, professorgandhi29@gmail.com
[2]Professor, Faculty of Computing, Sathyabama University, ac.christy@gmail.com

Abstract

Key management is vital part of security; this issue is even bigger in wireless network compared to wired network. The distribution of keys in an authenticated manner is a difficult task in WMANET and when a node leaves or joins it need to generate new session key to maintain forward and backward secrecy. This paper reviewed technological solutions for managing keys by divide the network into clusters. A clustering architecture increases network lifetime and fault tolerance, and results in more efficient use of network resources. Cluster head will maintain the group key, it will also update the group key whenever there is a change in the membership. And the CH is responsible for inter-cluster and intra-cluster communication. A Secondary Cluster Head (SCH) is also elected to avoid the CH from becoming a bottleneck, and also it acts a monitoring node for cluster head lifetime. The combination of Weight based Clustering and RSA algorithm has been proposed for secure multicast key distribution in which source node uses Ad hoc On-Demand Distance Vector (AODV) routing protocol to reach its destination. The weight based clustering approach is based on combined weight metric that takes into account of several system parameters like the degree difference, transmission range, battery power and mobility of the node. The performance of the system is evaluated based on the few metrics like Packet Delivery Ratio (PDR), and end to end delay. As demonstrated, our algorithm reduces frequent head election phenomena by having SCH, thus improving overall performance and reducing energy utilization.

Keywords: WMANETs, Cluster Head, Secondary Cluster Head, AODV, RSA

Introduction

Wireless Mobile Ad hoc Networks (WMANETs) are deployed in difficult environments where interruption of connectivity is consistent occurrences. Wireless

Mobile Ad hoc Networks (WMANETs) are infrastructure less, multi-hop, dynamic networks for a collection of heterogeneous mobile nodes. It consists of autonomous nodes that communicate with each other, most frequently using a multi-hop wireless network. Nodes do not necessarily know each other and come together to form an ad hoc group. Key management is a basic part of any secure communication. Secure group communication (SGC) is defined as the process by which members in a group can securely communicate with each other and the information being shared is inaccessible to outside members. In such a scenario, a group key is established among all the participating members and this key is used to encrypt all the messages destined to the group. As a result, only the group members can decrypt the messages. Due to dynamic behavior of the MANET, secret key used for communication is need to be updated whenever any node joins or leaves the network in order to maintain the forward and backward secrecy with in the network. If the network is large and the mobility is higher, key updation is a frequent phenomenon. It also consumes more battery power. In order to manage the energy utilization, a network is divided into clusters by using Weight based Clustering and the keys are generated using well known Group Diffie Hellman Exchange Algorithm. Here the re keying process will be performed only if there is any mobility of nodes in the clusters. The remainder of this paper is organized as follows. Section 2 presents related work done in Clustering and key management approaches. Section 3 presents the proposed Weight based Clustering and Group Key Agreement Section 4 presents performance evaluation and finally, Section 5 presents Conclusions and future work.

Related Work

Key management has remained a challenging issue in wireless networks due to the constraints of node resources. Majority of research on security of ad hoc networks emphasize the secure routing protocols, there are some proposals on key generation and distribution issues. At the same time key management will be tedious process when we have large network due to high mobility of nodes. To manage these issues, various cluster based routing schemes have been proposed in the literature namely low-maintenance clustering approach,[18] mobility-based clustering approach, Weight-Based Clustering approach, Flooding-Based Clustering approach, Channel Based Clustering. Clustering protocols are categorized into different approaches based on its distinguished features. Tree structure of key management approaches are as follows.

A. Types of key management

The group key management protocols are typically classified in four categories:

1) Centralized Group Key Distribution (CGKD),

In CGKD, there exists a central entity (i.e. a group controller (GC)) which is responsible for generating, distributing, and updating the group key e.g. Logical Key Hierarchy (LKH) and One Way Function (OFT)

2) De-Centralized Group Key Management (DGKM),
The DGKM approach involves splitting a large group into small subgroups. Each subgroup has a subgroup controller which is responsible for the key management of its subgroup .e.g. IOLUS

3) Distributed/Contributory group Key Agreement (CGKA)
The CGKA schemes involve the participation by all members of a group towards key management. Such schemes are characterized by the absence of the GC. The group key in such schemes is a function of the secret shares contributed by the members. Typical CGKA schemes include binary tree based ones [4] and n-party Diffie-Hellman key agreement [5, 6]. RSA is a group key management scheme proposed in [4]. The basic idea is to combine the efficiency of the tree structure with the contributory feature of DH.

B. Clustering protocols
Clustering protocols are categorized into different approaches based on its distinguished features

a) *Low-Maintenance Clustering* approach [3, 11-13] provides a stable cluster structure incurring less maintenance cost.

a) *Lowest-ID*: Elect the node as a cluster head that has the lowest ID relative to its neighbors
b) *Maximum Connectivity Clustering (MCC):* The MCC [14] uses the degree of connectivity instead of the node ID in the cluster head election.

b) *Mobility-Based Clustering* approach considers mobility feature of the mobile nodes forcluster formation. It achieves maximum cluster stability by grouping mobile nodes of similar patterns into a single cluster.

a) *MOBIC***:** uses the mobility metric as a basis of cluster formation and cluster head selection.

c) *Weight-Based Clustering* approach takes weight of the mobile nodes into consideration for the choice of the cluster head.

a) On-Demand Weighted clustering algorithm (On- Demand WCA) The assignment of weight to a mobile node is the combined effect of several system parameters like ideal node degree, degree difference, transmission power, cluster head serving time and mobility. The advantage of this clustering scheme is the flexibility of adjusting the weighting factors for each system parameter to make it suitable for different scenarios.

d) *Flooding-Based Clustering* approach forms the cluster by disseminating information over the whole network

a) *Max min D-cluster algorithm [6]: This* allows the control and flexibility in the determination of the cluster head density by generalizing the distance of a mobile node from its cluster head to be d hops

5) Channel Based Clustering facilitates efficient utilization of channels by scheduling transmissions of the mobile nodes.

Proposed Work

In our proposed work, the combination of Weight based Clustering and RSA algorithm for secure multicast key distribution is applied , in which source node uses Ad hoc On-Demand Distance Vector (AODV) routing protocol to reach its destination. The Cluster Head is responsible for cluster management, membership maintenance and Group Key Distribution and updation. Initially, all the nodes are assigned an id, its private key and public key. Cluster Head is selected based on Weight Based Algorithm by using various metrics. The reason behind using Weight-Based Clustering approach in this paper takes weight of the mobile nodes into consideration for the choice of the Cluster Head.

The Weight based clustering approach is based on combined weight metric that takes into account of several system parameters like the degree difference of the node, transmission range, battery power and mobility of the node. But in existing clustering algorithms like MCC, MOBIC and lowest ID, any one of the weight metric is used for electing the CH. Re keying is done by Cluster Head whenever any node joins or leaves the network to ensure backward secrecy (i.e., a new member should not know the previous information that was exchanged) and forward secrecy (i.e., an existing member should not receive the information exchanged after it eaves the network)

Key management is an essential cryptographic primitive upon which other security primitives such as privacy, authenticity and integrity are built. However, none of the existing key management schemes are suitable for ad hoc networks. The major limitation of these schemes is that most of them rely on a Trusted Third Party (TTP), thus not fulfilling the self-organization requirement of an ad hoc network. Special mechanisms and protocols designed specifically for ad hoc networks are necessary. For this reason, Distributed/Contributory group Key Agreement (CGKA) approach is used for establishing the group key by the contribution of cluster members.

A. Phases in Clustering and key management

The key management system consists of two phases

1) Initialization (Weight Computation, Cluster Head Election and Formation)

1) Initialization phase

Initially weight will be computed for every node based on the factors like degree difference of the node, transmission range, and battery power and mobility of the sensor node. This module consists of following sub modules like Cluster Head election and cluster formation.

a) Weight Computation

Initially each node is assigned a random ID value. It broadcasts its ID value to its neighbors and builds its neighborhood table. Each node calculates its own weight based on the following factors like Node degree difference, Energy remaining, Mobility, distance from all other neighboring nodes. The distance between nodes and mobility is considered to keep the balance between clusters. The weight computation W for all the weights is given as follows in equation (1).

$$W_n = W_1 * \Delta_n + W_2 * E_n - W_3 * M_n + W_4 * D_n \text{ -----} \quad (1)$$

Where Δ_n – Degree Difference of node

E_n -Energy in each node represented by Joules

M_n - Mobility of each node. (Less mobility nodes have more probability to become a CH)

D_n - Distance from all other neighboring nodes

The co-efficient used in weight calculations W_1, W_2, W_3, W_4 are assumed as follows. $W_1 = 0.5, W_2 = 0.35, W_3 = 0.05, W_4 = 0.1$. The sum of these co-efficient is 1. The factors degree difference and energy are given more importance and assumed higher co-efficient values 0.5 and 0.35. The combined weight is calculated by using the parameters of Δ_n, E_n, M_n, D_n from the equations 2,3,4,5 respectively. After finding its own weight, each node broadcasts its weight to its neighbors based on neighborhood table. The neighborhood table consists of one hop reachable nodes; its weights. It is maintained by the CH.

Degree difference

It is defined as the difference between the cluster size N and the actual number of neighbours d_n.From the equation (2), it is known that Δ_n – Degree Difference of node 'n'. In order to find the Degree d_n of the node 'n' by counting its neighbors. Compute the Degree difference for the node 'n', where N is a threshold for the cluster's size.

$$\Delta_n = \left| d_n - N \right| \text{ ----------} \quad (2)$$

Energy

Energy in each node represented by Joules. It is represented by E_n - Energy (Battery Power) of node 'n'. Energy E_n is calculated as

$$E_n = E_0 - E_{residual} \text{ ----------} \quad (3)$$

E_0 and $E_{residual}$ are initial and remaining energy of node 'n'

Mobility of each node

Less mobility nodes have more probability to become a CH. It is represented by M_n - Mobility (Speed) of each node. It is calculated as

M_n - Mobility speed of every node by following formula

$$M_n = \frac{1}{T} \sum_{t=1}^{T} \sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2} \text{ ----------} \quad (4)$$

Where (X_t, Y_t) and (X_{t-1}, Y_{t-1}) are the co-ordinate positions of node 'n' at time t and t-1, T= cumulative time.

Distance

Distance from all other neighboring nodes is represented by D_n .Here; the sum of the distance between member nodes and its neighbors *is* defined by the equation (5). In order to find the neighbor $N(n)$ of each node 'n', the D_n is calculated as

$$D_n = \sum_{n' \in N(n)} distance(n, n') \quad \text{----------} \quad (5)$$

D_n - The sum of the distances between node 'n' with its entire neighbor.

b).Cluster Head Election And Cluster Formation

Here the Cluster Head election and Cluster Head lifetime monitoring algorithm are discussed.

ALGORITHM FOR CLUSTER HEAD ELECTION

Step 1:

Calculate weight for every node based on the metrics like Node Degree, Mobility, Connectivity and Energy Remaining.

Step 2 :

Broadcast Weight value and its Id to all its neighboring nodes and the neighborhood table updated with weight value

Step 3:

Cluster Head (CH) and Secondary Cluster Head (SCH) elected based on the weight value

If (The Node with highest weight value)

Elect that Node as a CH

If (The Node with next highest weight)

Elect that Node as a SCH

Else

Ordinary nodes send Join Request to CH to form a Cluster

Figure 1: Algorithm For Cluster Head Election

.

ALGORITHM FOR CLUSTER HEAD LIFETIME

Step 1:

SCH monitor the battery level of CH for every 30s

If (Battery level of CH< Minimum Threshold Level)

SCH will become New CH, Send CH_LIFE DOWN Msg to all member nodes, Election procedure iniated to find new SCH

Else

Re election not needed;

Figure 2: Algorithm For Cluster Head Lifetime

B. Group Key Agreement (Generation & Distribution)

1) Group Key Generation And Distribution

After Weight Computation and cluster formation, members in the clusters will send its id and public key. Cluster Head receive the message and initiate the group key calculation by using RSA. It uses the member's Public Key to calculate group key as follows.

$$CH : GK = ((\alpha)^{pk1+\ pk2+\ldots pKn\ +CH_k} \bmod p)\ X\ (R_v) \text{ ----------} \quad (1)$$

GK- Group Key

Where

α – primitive root of p

CH_k – secret key of cluster head,

pk1,pk2 …pkn – public keys of individual nodes ithin the cluster,

p – prime number

R_v – secret random value generated every time while re-keying.

ALGORITHM FOR THE GK GENERATION

Step 1 :

If (Node present within the cluster)

if CH gets public keys of all nodes
calculate group key as follows:

CH : GK =((α) $^{pk1+\ pk2+\ldots pKn\ +CH_k}$ mod p) X (R_v)

End if

End if

Figure 3: Algorithm for the GK generation

ALGORITHM - ENCRYPTION AND DECRYPTION FOR KEY DISTRIBUTION

Step 1:

CH → nodes within the cluster
Encrypt using : E (GK)
RSA algorithm where
E(GK) = ((GK) e mod n) in which
{e, n} are public key pair.

Step 2:

Decrypt Nodes: D(GK) = (E(GK)d mod n)
in which {d,n} are private key pair.

Figure 4: Algorithm - encryption and decryption for key distribution

The distribution of group key is done using RSA algorithm. Cluster head having (e,n) public key and every node maintains (d,n) private key. When ever any new node joins into the cluster, Cluster Head calculates new group key and multicast to already existing nodes. And Cluster Head unicast the group key to new node along with private key for RSA algorithm.

Simulation Results and Discussions

The number of nodes used in the simulation results varies between 20 and 100. The simulations were run for 300 seconds. The cluster size was fixed at 15. We depict some statistics on the formed clusters for different transmission ranges. In the first set of simulations, the scalability of the algorithm is measured in terms of nodes density

and transmission range. In this paper, the NS-2 simulator [15] is used for the simulation.

The total energy consumption and Packet Delivery Ratio of total network are compared between without and with clusters.

A. *Packet Delivery Ratio (PDR)*

Data Packet Delivery Ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by Destination.

PDR = No. of Packets Sent/ No. of Packets Received

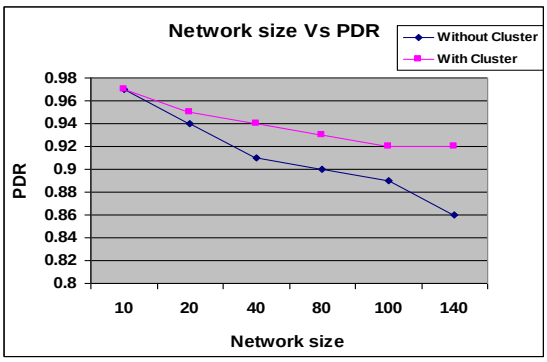

Figure 5: Network size Vs PDR

Fig.5 is the total Packet Delivery Ratio (PDR) of entire Network nodes. The difference in the delivery ratios increases as the network's size increases, which shows the performance gained because of Weight based Clustering scheme.

B. Total Energy consumption

Fig.6 is the total energy consumption of entire network nodes. Initially both the protocols consuming energy almost the same but after time of 400, there is a change in energy consumption of two protocols. So, the proposed protocol weighted Clustering algorithm which can save more energy better than other Clustering algorithms.

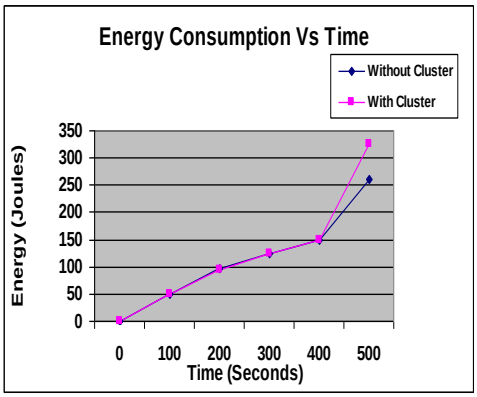

Figure 6: Energy Consumption Vs Time

Conclusion

This approach is based on combined weight metric that takes into account of several system parameters like the degree difference of the node, transmission range, battery power and mobility of the sensor node. Since energy utilization is the most important criteria in cluster based routing schemes, our protocol provides better results than existing Lowest-id, WCA algorithm and LEACH algorithm. Performance metrics like network size with Packet delivery Ratio, Energy Consumption have been evaluated between with clustering and without clustering. In the near future, some other performance metrics like fault tolerance can be taken for performance evaluation and this protocol can be extended to include group key management for inter clustering to provide secure transmission of collected data. We also intend to extend the clustering architecture to support multi-hop clustering in Wireless mobile adhoc networks (WMANs). Effective utilization of power, Bandwidth wastage helps in improving the quality of service in WMANs by applying the Weighted Clustering Algorithm.

References

[1] Anitha, V.S., Sebastian, M.P.(2009), "SCAM: Scenario-based clustering algorithm for mobile *ad hoc* networks ", in Proceedings of the 13th IEEE/ACM International Symposium on Distributed Simulation and Real-Time Applications, pp. 97-104.

[2] Basagni, S. et al (2006), "Localized protocols for *ad hoc* Clustering and backbone formation: A performance comparison", IEEE Trans. Parall. Distrib. Sys. 2006, 17, pp. 292-306.

[3] Dhurandher, S.K.; Singh, G.V (2005), "Weighted-based adaptive clustering algorithm in mobile ad hoc networks ". in Proceedings of ICPWC'2005, New Delhi, India, pp. 96-100.

[4] K. Akkaya and M. Younis, (2003) "A Survey of Routing Protocols in Wireless Sensor Networks", Elsevier Ad Hoc Network Journal, 3(3), pp .325-349.

[5] LI Fangmin et al (2008), "Power Control for Wireless Sensor Networks", Journal of Software Engineering, 19(3): pp. 716−732

[6] Q. Jiang and D. Manivannan(2004), "Routing protocols for sensor networks", in Proc.1st IEEE Consumer Comm. & Net. Conf. (CCNC), pp. 93-98.

[7] Zhang Jian-wu et al, (2008), "Weighted Clustering Algorithm Based Routing Protocol in Wireless mobile adhoc sensor networks (WMASNs)",

[8] Sanjay kumar padhi et al (2008), "Review of routing protocols in sensor and Adhoc networks ", International journal of reviews in computing

[9] Adeel Akhtar, Abid Ali Minhas, and Sohail Jabbar (2010) "Energy Aware Intra Cluster Routing for Wireless Mobile Adhoc Sensor Networks (WMASNs) ", International Journal of Hybrid Information Technology Vol.3, No.1, pp. 29-48

[10] Naveen chauhana (2011), "Distributed Weighted Cluster Based Routing Protocol for MANETS" w*ireless Sensor Network*, 2011, 3, pp. 54-60.

[11] Tzung-Pei Hong et al (2011), "An Improved Weighted Clustering Algorithm for Determination of Application Nodes in Heterogeneous Sensor Networks", Journal of Information Hiding and Multimedia Signal Processing, Ubiquitous International, Volume 2, Number 2, pp. 173- 184.

[12] R. Pandi Selvam et al (2011), "Stable and Flexible Weight based Clustering Algorithm in Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 2 (2), pp. 824-828.

[13] Jutao Hao et al (2011), "Energy Efficient Clustering Algorithm for Data Gathering in Wireless Sensor Networks", Journal of Networks, Vol. 6, no. 3, pp. 490 - 497.

[14] Huiheng Liu et al (2011), "Cooperative Spectrum Sensing and Weighted-Clustering Algorithm for Cognitive Radio Network", I.J. Information Engineering and Electronic Business, vol. 2, pp. 20-27.

[15] NS-2 simulator. Available online: http://www.isi.edu/nanam/ns (17 May 2011)

[16] Maneesha V.Ramesh ,Abishek T.K, Aparnadhusoodanan, Wireless Sensor Network Based Localization Scheme for Tracking Emergency Responders in Disaster Area ICWCA-2011 ,Aug 01-03,2011.

[17] H. Bettahar, A. Bouabdallah, and Y. Challal,"An adaptive key management protocol for secure multicast," in 11th International Conference on Computer Communications and Networks ICCCN, Florida USA, Oct. 2002.

[18] M. S. Bouassida, I. Chrisment, and O. Festor, "An enhanced hybrid key management protocol for secure multicast in Ad Hoc networks," in Networking 2004, Third International IFIP TC6 Networking Confer-ence, LNCS 3042, pp. 725-742, Springer, May 2004.

[19] M. S. Bouassida, I. Chrisment, and O. Festor, "Efficient clustering for multicast key distribution in MANETs," in Networking 2005, International IFIP TC6 Networking Conference, LNCS 3462, pp. 138-153, Springer, May 2005.

[20] Y. Challal, H. Bettahar, and A. Bouabdallah, "SAKM: A scalable and adaptive key management approach for multicast communications," ACM SIG- COMM Computer Communications Review, vol. 34,no. 2, pp. 260-271, Apr. 2004.