A Cluster Tree Based Model for Secure Data Retrieval in Military using Wireless Sensor Networks

Mrs. J. Sreemathy[1]
Department of Computer Science and Engineering
SRI Eswar College of Engineering
Coimbatore, India
jsreemathybe@gmail.com

Mr.N.Prasath[2], Mr. M.Saravanan[3]
Department of Computer Science and Engineering
KPR Institute of Engineering and Technology
Coimbatore, India
n.prasath@kpriet.ac.in[2]
m.saravanan@kpriet.ac.in[3]

Abstract**—** Wireless sensor networks (WSNs) can be used in military environments such as a battlefield tracking the enemies. One of the challenging issues in this scenario is enforcement of authorization policies and the policies update for secure data retrieval. CP-ABE is using efficient and secure data retrieval method for decentralized DTNs. However implementing Cipher text-Policy Attribute – Based Encryption (CP-ABE) in decentralized DTNs where the key authorities might be compromised or not fully trusted. In this paper we propose a secured data retrieval method using Cluster Tree Based Model proposes grouping the slave nodes, where each node has an individual group head. The cluster model provide key to group head and the group head will distribute the key to all members and implementing Position-based Aggregator Node Election protocol (PANEL) is a position-based clustering routing protocol for WSNs. The main goal of PANEL is to elect aggregators, i.e., CHs. PANEL protocol are used to balance the network node load pressure and reduces the communication load.

Keywords*- Wireless sensor networks, Cipher text-policy attribute-based encryption, Position-based Aggregator Node Election protocol, Clustering, Cluster Head.*

*****

I. Introduction

Sensor networks are deployed for applications such as wildlife habitat monitoring, Forest fire prevention and military surveillance [9]-[11]. In these applications, the data collected by sensor a node from their physical environment needs to be collected at host computer for further analysis.

In many network scenarios, connections of wireless devices carried may be disconnected by many environmental factors and mobility, especially when they operate in aggressive environments. Disruption-tolerant network (DTN) technologies are successful solutions that allow nodes to communicate with each other in these intense networking environments [1]–[3].

Roy [4] and Chuah [5] introduced storage nodes in DTNs where data is replicated such that only authorized nodes can access the necessary information quickly and efficiently. Applications such as military surveillance require increased protection of confidential data including access control techniques that are cryptographically enforced [6], [7]. In many cases, it is popular to provide distinguish right to use services such that data access strategy are defined over user attributes or roles, which are managed by the key authorities. By referring to this DTN architecture where multiple authorities issue and manage their own attributes keys independently as a decentralized DTN.

The problem of applying the ABE to DTNs introduces several security and privacy challenges. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys [8].

We propose a Cluster Tree Based Model proposes grouping the soldier's nodes, where each node has an individual group head. The cluster model provide key to group head and the group head will distribute to all members. Position-based Aggregator Node Election protocol (PANEL) is a position-based clustering routing protocol for WSNs.

II. Related Work

1) Attribute Revocation
Bethencourt et al. [12] and Boldyreva et al. [14] first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes [8], [12], [14], [15] have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy [16]. The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the nonrevoked users can update their keys. This results in the "1-affects- " problem, which means that the update of a single attribute affects thewhole nonrevoked users who share the attribute [17].

2) Key Escrow

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information [11], [12], [13], [18]–[20]. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

3) Decentralized ABE:

Huang et al. [9] and Roy et al. [4] proposed decentralized CP-ABE schemes in the multi authority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times.

4. CP-ABE for decentralized DTNs

Junbeom Hur and Kyungtae Kang [8] proposed First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access str

ucture under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture.

III. Proposed Work

A. *PANEL protocol*

Assumes that the sensor nodes are deployed in a bounded area, and this area is partitioned into geographical clusters. The clustering is determined before the deployment of the network, and each sensor node is pre-loaded with the geographical information of the cluster which it belongs to. In our simplified case, each sensor node is pre-loaded with the coordinates of the lower-left corner of its cluster, as well as with the size d of the cluster.

In addition, as we mentioned before, each node i is aware of its own geographical position ~Pi. PANEL also includes a position-based routing protocol that is used in inter-cluster communications. As the nodes are aware of their geographical position, this seems to be a natural choice that does not result in additional overhead. The position-based routing protocol is used for routing messages from a distant base station or from a distant aggregator towards the reference point of a given cluster.

PANEL supports asynchronous sensor network applications where the sensor node readings are fetched by the BSs. PANEL communications is used to establish routing tables for intra-cluster routing. The intra-cluster routing is used to route a message to the aggregator of a given cluster if that messages are already inside the cluster. The main goal of PANEL is to elect aggregators, i.e., CHs.

PANEL protocol is used to balance the network node load pressure and reduces the communication load.

B. *SYSTEM ARCHITCTURE*

1. Node Identification and Communication

• Disruption-tolerant network (DTN) technologies are becoming successful solutions that identify the nodes and to communicate with each other in these extreme networking environments.

• Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.

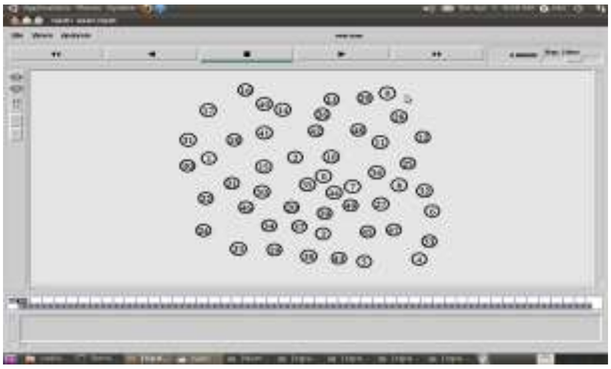

Figure1. Creation of Nodes

2. Clustering the nodes

- It proposes a novel clustering method to limit the number of member nodes for each cluster head by using a key value.
- The revocation of any attribute or any single user in an attribute group would affect the other users in the group.

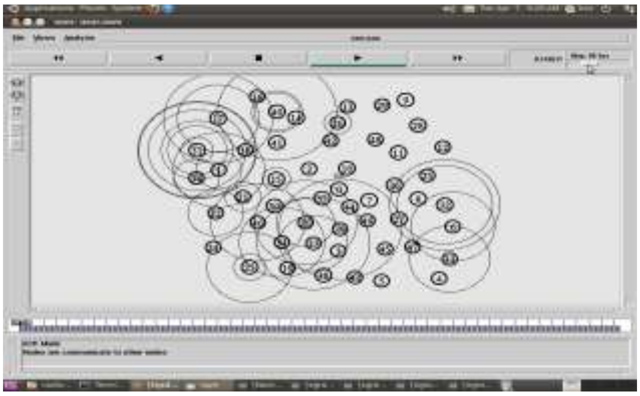

Figure2. Node communication with other nodes via BS

3. Data Distribution

- When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively.

- The key Distribution procedure is launched by sending a join or leave request for some attribute group from a user who wants to hold or drop the attribute to the corresponding authority. On receipt of the membership change request for some attribute groups, it notifies the storage node of the event.

4. Data Retrieval

The stored data can be launched by the storage node and the key authorities. Since they cannot be totally trusted, confidentiality for the stored data against them is another essential security criteria for secure data retrieval in DTNs. An efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.

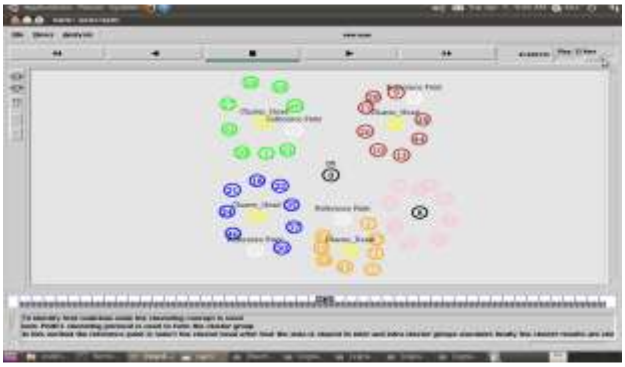

Figure3. Clustering the Node

- The local authorities issue a set of attribute keys for their managing attributes to an authenticated user .If the storage node manages the attribute group keys; it cannot decrypt any of the nodes in the access tre**e** in the cipher text. This is because it is only authorized to re encrypt the cipher text with each attribute group key.
- Therefore the data retrieval process gives data confidentiality against the curious key authorities and storage node is also ensured. It provides differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities.

5. Identifying the malicious node

Clusters are formed from available nodes each cluster has their own cluster head and reference point based on cluster formation the malicious nodes are identified from each cluster. The cluster group is formed with the help of PANEL clustering protocol.

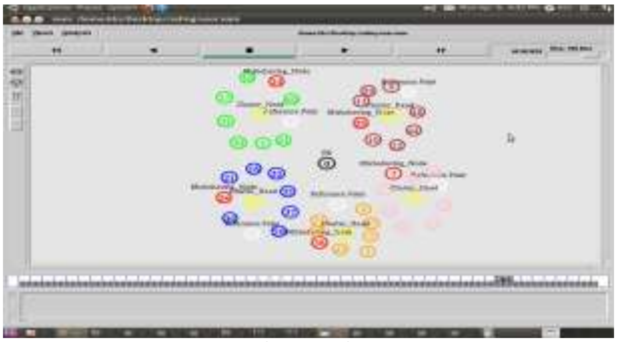

Figure4. Identification of malicious node

6. Removing the malicious node

In this method reference point is used to select the cluster head after that the data is shared with inter and intra cluster groups members finally the cluster results are checked and the base station gives the malicious node report.

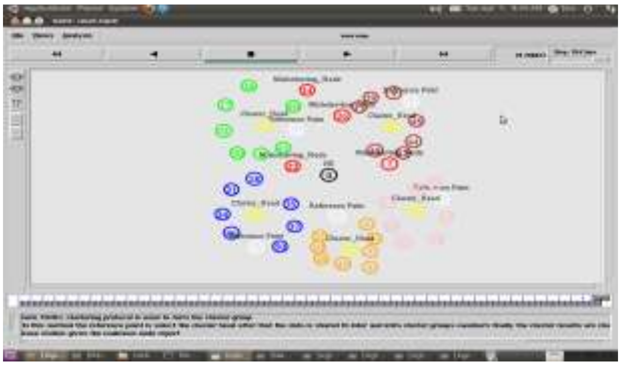

Figure5. Removing the malicious node

IV. Simulation and Result Analysis

A. *Packet Delivery Ratio*

The packet delivery ratio of PANEL is very high when it was compared to the other techniques that prevailed previously. The packet delivery ratio is approximately 19.8000*106 in PANEL and in AODV it was approximately 3.0000*10^6 and in DSR it was approximately 2.0000*10^6.

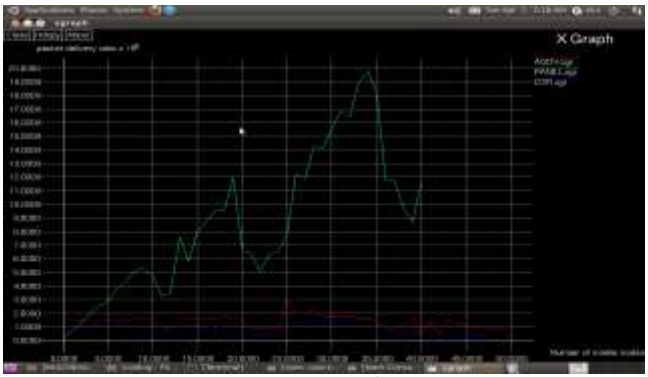

Figure6. Comparing packet delivery ratio of PANEL protocol with AODV and DSR.

B. *Throughput*

The Throughput of work PANEL is very high when it was compared to the other techniques that prevailed previously. The Throughput is approximately 1.6*10^6 in PANEL and in AODV it was approximately 1.3*10^6 and in DSR it was approximately 0.5*10^6.

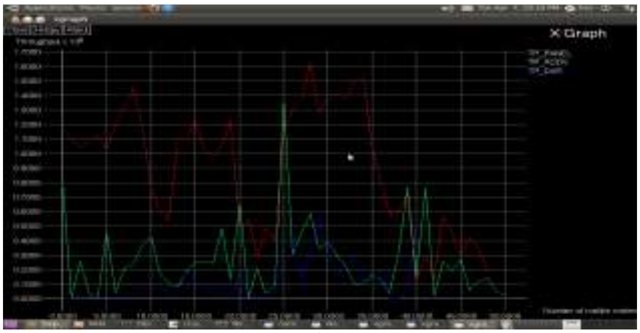

Figure7. Comparing throughput of PANEL protocol with AODV and DSR.

C. *Delay*

The delay in PANEL is low when compared to other technology and it is approximately 0.8000*10^6 .

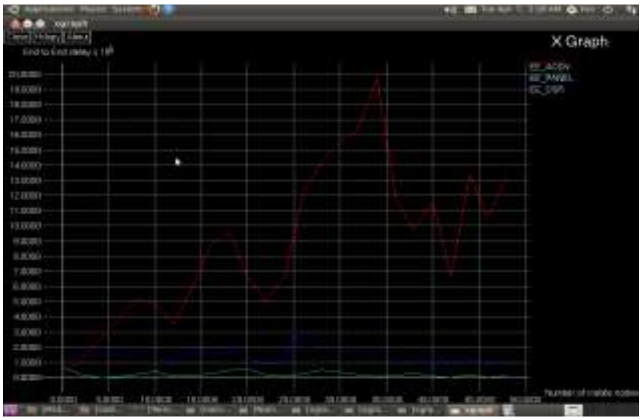

Figure7. Comparing throughput of PANEL protocol with AODV and DSR.

V. CONCLUSION AND FUTURE WORK

Cluster tree model (PANEL) are becoming successful solutions in military applications as they allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. Possibilities of adopting cluster-based technology in further reduce the delay and to find the mismatch of data So that the confidential data can be distributed securely and efficiently in the disruption tolerant military network. To increase the merits of our research work, we plan to investigate the following issues in our future research:

- Various other cryptography techniques can be used to further reduce the network overhead and data can be securely transferred.
- Cluster head can be changed periodically so that the data remains secure and can be transferred confidentially.

.REFERENCES

[1] Almeroth .K. C and M. H. Ammar, “Multicast group behavior in the Internet’s multicast backbone (MBone),” *IEEE Commun. Mag.*, vol.35, no. 6, pp. 124–129, Jun. 1997.

[2] Bethencourt,.J A. Sahai, and B. Waters, “Cipher text-policy attribute based Encryption,” in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[3] Burgess.J, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for vehicle based disruption tolerant networks,” in Proc. IEEE INFOCOM, 2006, pp. 1–11.

[4] Boldyreva.J, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[5] Chase.M and S. S. M. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.

[6] Cheung.L and C. Newport, “Provably secure cipher text policy ABE,” in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[7] Goyal.L, A. Jain,O. Pandey, andA. Sahai, “Bounded ciphertext policy Attribute-based encryption,” in Proc. ICALP, 2008, pp. 579–591.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, “Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption,” in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[9] D. Huang and M. Verma, “ASPE: Attribute-based secure policy enforcement in vehicular ad hoc

networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

[10] Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" in IEEE/ACM transactions on networking, vol. 22, no. 1, February 2014.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[13] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195–203.

[14] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.

[15] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in Proc. ACMConf. Comput. Commun. Security, 2006, pp. 99–112.

[16] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.

[17] S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.

[18] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.

[19] M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp. 515–534.

[20] S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.

[21] M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp. 515–534.