Privacy Preserving and Secure Data Retrieval in Sensor Network using Homomorphic Encryption Algorithm

*1S.Shanmugasundaram and #2S.Chitra

*M.Tech, Dept of CSE, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry

#Asst Professor, Dept of CSE, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry

1shanmugasundaram91@gmail.com

***Abstract*— The Cipher text-policy Attribute Based Encryption for secure data retrieval in decentralized Disruption Tolerant Networks (DTNs) where multiple key authorities manage their attributes independently. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized Disruption Tolerant Networks architecture proposed a decentralized approach; their technique does not authenticate users. Demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. Finally the Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. We propose an efficient system for preventing location leaks in Sensor Networks and also it ensures the privacy-preserving scheme against traffic analysis and flow tracing. With the faster homomorphic encryption algorithm technique, the proposed scheme offers two significant privacy preserving features, packet flow untraceability and message content confidentiality, which can efficiently thwart traffic analysis/flow tracing attacks. Moreover, with homomorphic encryption, the proposed scheme keeps the essence of random linear network coding, and each sink can recover the source messages by inverting with a very high probability. Our Proposed system works efficiently when compared to previously existing schemes.**

Index Terms—Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multi authority, secure data retrieval, privacy preserving, homomorphic encryption algorithm

I. Introduction

Nowadays A fundamental characteristic [1] of wireless ad hoc networks is the time difference of the channel potency of the original communication links. Such time difference occur at numerous occasion scales and can be owing to multipath desertion, pathway loss using space attenuation, shadowing by obstacles, and intrusion from extra users. The impact of such time difference on the design of wireless ad hoc networks permeates throughout the layers, ranging from coding and power control at the physical layer to cellular handoff and coverage planning at the networking layer. An important means to cope with the time variation of the channel is the use of diversity. The basic design is to recover presentation by creating numerous autonomous signal ways flanked by the source and the target nodes. These diversity modes pertain to a point-to-point link. Recent results point to another form of diversity, inherent in a wireless network with multiple users. Overall system throughput is maximized by allocating at any time the common channel resource to the user that can best exploit it. Similar results can be obtained for the downlink from the base station to the mobile users.

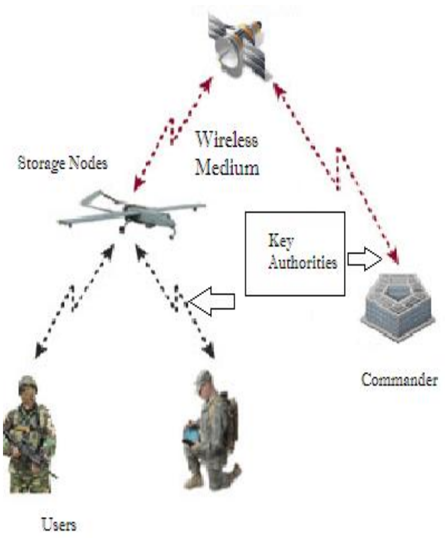


Figure 1 Military Delay Tolerant Networks Model

The wireless networks are classified into different types: Mobile ad-hoc networks, Sensor network, Delay Tolerance Networks, and so on. In this paper we discuss about Delay Tolerant network in military application network for communication. We introduce encryption concepts in military networks for to prevent the communication messages from hackers or attacks. The concept of attribute-based encryption (ABE) is a promising approach that fulfils the requirements for se-cure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to de-crypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy.

There are many existing system are proposed previously to address security issues in delay tolerance networks. In existing system, Attribute Based Encryption 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. 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.

The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. An Attribute Based Encryption is to improve upon the scalability of the above solutions; one-to-many encryption methods such as Attribute Based Encryption can be used. In order to overcome the following disadvantages in previous works: Key escrow problem in a multi-authority system, one-to-many encryption methods and Attribute revocation problems. We proposed Cipher text Policy Attribute Based Encryption (CP-ABE) for secures data retrieval in disruption tolerant military network. In a cipher text policy attribute-based encryption scheme, each user’s private key is associated with a set of attributes representing their capabilities. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing vulnerability. In this paper, we attempt to enhance the existing secure date retrieval model of decentralized disruption tolerant military networks with providing Source Anonymity. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic. Known as the source anonymity problem, this problem has emerged as an important topic in the security of wireless sensor networks, with variety of techniques based on different adversarial assumptions being proposed. In this work, we present a new framework for modelling, analyzing, and evaluating anonymity with enhanced secure date retrieval for decentralized disruption-tolerant military networks.

The rest of the paper will be organised as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The implementation of our paper is in section 4. Our proposed system algorithm is in section 5. In Section 6, conclusion and Future work of our system.

II. Related work

As a promising communication paradigm, Cognitive Radio Networks (CRNs) have paved a road for Secondary Users (SUs) to opportunistically exploit unused licensed spectrum without causing unacceptable interference to Primary Users (PUs). In this paper, we study the distributed data collection problem for asynchronous CRNs, which has not been addressed before. First, we study the Proper Carrier-sensing Range (PCR) for SUs. By working with this PCR, an SU can successfully conduct data transmission without disturbing the activities of PUs and other SUs. Subsequently, based on the PCR, we propose an Asynchronous Distributed Data Collection (ADDC) algorithm with fairness consideration for CRNs. ADDC collects data of a snapshot to the base station in a distributed manner without any time synchronization requirement. The algorithm is scalable and more practical compared with centralized and synchronized algorithms. Through comprehensive theoretical analysis, we show that ADDC is order-optimal in terms of delay and capacity, as long as an SU has a positive probability to access the spectrum. Finally, extensive simulation results indicate that ADDC can effectively finish a data collection task and significantly reduce data collection delay.

The purpose of a wireless sensor network (WSN) is to provide the users with access to the information of interest from data gathered by spatially distributed sensors. Generally the users require only certain aggregate functions of this distributed data. Computation of this aggregate data under the end-to-end information flow paradigm by communicating all the relevant data to a central collector node is a highly inefficient solution for this purpose. An alternative proposition is to perform in-network computation. This, however, raises questions such as: what is the optimal way to compute an aggregate function from a set of statistically correlated values stored in different nodes; what is the security of such aggregation as the results sent by a compromised or faulty node in the network can adversely affect the accuracy of the computed result. In this paper, we have presented an energy-efficient aggregation algorithm for WSNs that is secure and robust against malicious insider attack by any compromised or faulty node in the network. In contrast to the traditional snapshot aggregation approach in WSNs, a node in the proposed algorithm instead of unicasting its sensed information to its parent node, broadcasts its estimate to all its neighbors. This makes the system more fault-tolerant and increase the information availability in the network. The simulations conducted on the proposed algorithm have produced results that demonstrate its effectiveness.

Sensor networks are collection of sensor nodes which co-operatively send sensed data to base station. As sensor nodes are battery driven, an efficient utilization of power is essential in order to use networks for long duration hence it is needed to reduce data traffic inside sensor networks, reduce amount of data that need to send to base station. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks (WSN) offer an increasingly Sensor nodes need less power for processing as compared to transmitting data. It is preferable to do in network processing inside network and reduce packet size. One such approach is data aggregation which attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity. Wireless sensor networks have limited computational power and limited memory and battery power, this leads to increased complexity for application developers and often results in applications that are closely coupled with network protocols. In this paper, a data aggregation framework on wireless sensor networks is presented. The framework works as a middleware for aggregating data measured by a number of nodes within a network. The aim of the proposed work is to compare the performance of TAG in terms of energy efficiency in comparison with and without data aggregation in wireless sensor networks and to assess the suitability of the protocol in an environment where resources are limited.

Wireless Sensor Network is a field of research which is viable in every application area like security services, patient care, traffic regulations, habitat monitoring and so on. The resource limitation of small sized tiny nodes has always been an issue in wireless sensor networks. Various techniques for improving network lifetime have been proposed in the past. Now the attention has been shifted towards heterogeneous networks rather than having homogeneous sensor nodes in a network. The concept of partial mobility has also been suggested for network longevity. In all the major proposals; clustering and data aggregation in heterogeneous networks has played an integral role. This paper contributes towards a new concept of clustering and data filtering in wireless sensor networks. In this paper we have compared voronoi based ant systems with standard LEACH-C algorithm and MTWSW with TWSW algorithm. Both the techniques have been applied in heterogeneous wireless sensor networks. This approach is applicable both for critical as well as for non-critical applications in wireless sensor networks. Both the approaches presented in this paper outperform LEACH-C and TWSW in terms of energy efficiency and shows promising results for future work.

Wireless Sensor Networks have a wide range of applications including environmental monitoring. These networks consist of wireless sensor nodes which are densely deployed to provide a wider coverage area. The dense deployment of the sensor node provides spatial correlation in the network. In this paper an efficient data gathering approach is implemented by combining the dual prediction and clustering algorithm. Clustering algorithm based on spatial correlation is used to cluster the sensor nodes. Then within the cluster, the nodes send their data to the sink using the Normalized Least Mean Square dual prediction algorithm. Simulation results show that the proposed algorithm reduces the average energy consumption of the network.

In wireless sensor network [7], data fusion is considered an essential process for preserving sensor energy. Periodic data sampling leads to enormous collection of raw facts, the transmission of which would rapidly deplete the sensor power. In this paper, we have performed data aggregation on the basis of entropy of the sensors. The entropy is computed from the proposed local and global probability models. The models provide assistance in extracting high precision data from the sensor nodes. We have also proposed an energy efficient method for clustering the nodes in the network. Initially, sensors sensing the same category of data are placed within a distinct cluster. The remaining unclustered sensors estimate their divergence with respect to the clustered neighbors and ultimately join the least-divergent cluster. The overall performance of our proposed methods is evaluated using NS-2 simulator in terms of convergence rate, aggregation cycles, average packet drops, transmission cost and network lifetime. Finally, the simulation results establish the validity and efficiency of our approach.

Wireless sensor networks [3] (WSNs) are more likely to be d-distributed asynchronous systems. In this paper, we investigate the achievable data collection capacity of realistic distributed asynchronous WSNs. Our main contributions include five aspects. First, to avoid data transmission interference, we derive an $\Re 0$-proper carrier-sensing range ($\Re 0$-PCR) under the generalized physical interference model, where $\Re 0$ is the satisfied threshold of data receiving rate. Taking $\Re 0$-PCR as its carrier-sensing range, any sensor node can initiate a data transmission with a guaranteed data receiving rate. Second, based on $\Re 0$-PCR, we propose a Distributed Data Collection (DDC) algorithm with fairness consideration. Theoretical analysis of DDC surprisingly shows that its achievable network capacity is order-optimal and independent of network size. Thus, DDC is scalable.

Third, we discuss how to apply ℜ0-PCR to the distributed data aggregation problem and propose a Distributed Data Aggregation (DDA) algorithm. The delay performance of DDA is also analyzed.

Yih-Chun Hu, Adrian Perrig and David B. Johnson [4], as mobile ad hoc network applications are deployed; security emerges as a central requirement. In this paper we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. We present a new, general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes.

III. Proposed System

In our proposed system using Cipher text Policy Attribute Based Encryption (CP-ABE) for secures data retrieval in disruption tolerant military network.

In a cipher text policy attribute-based encryption scheme, each user's private key is associated with a set of attributes representing their capabilities. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing vulnerability.

Key escrow problem is resolved in the military network. 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 ciphertext addressed to specific users by generating their attribute keys.

Cipher text-Policy Attribute Based Encryption (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the descriptor needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy.

In this paper, we attempt to enhance the existing secure date retrieval model of decentralized disruption tolerant military networks with providing Source Anonymity. Mobile nodes in certain applications like the locations of events reported by a sensor network need to remain anonymous. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic. Known as the source anonymity problem, this problem has emerged as an important topic in the security of wireless sensor networks, with variety of techniques based on different adversarial assumptions being proposed. In this work, we present a new framework for modeling, analyzing, and evaluating anonymity with enhanced secure date retrieval for decentralized disruption-tolerant military networks.

Advantage

- Can be securing data retrieval decentralized DTN enhance CP-ABE.
- Using secret keys to decrypt the stored information.
- Data confidentiality.
- Collusion resistance.
- Backward and forward secrecy

System Model:

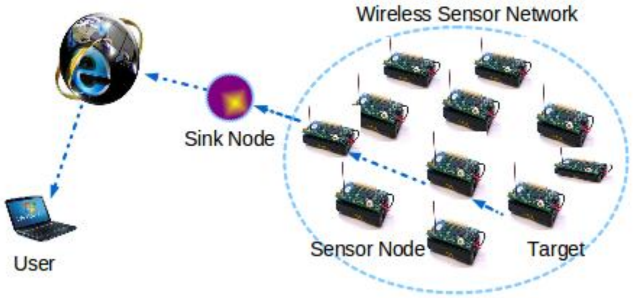


Figure 2 Our Proposed System Model

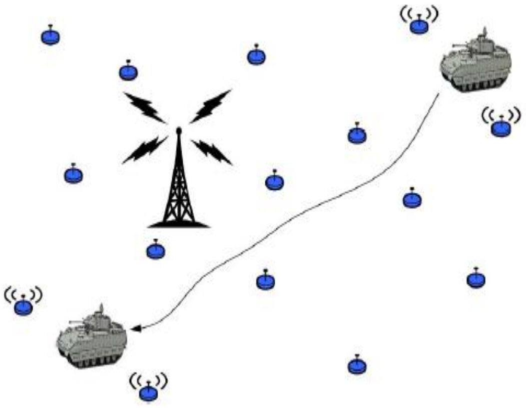


Figure 3 Application Scenario

IV. Implementation

There are five modules involved in the proposed work for secure data retrievals in disruption tolerant military network.

1. Attackers Modules
2. Privacy-Preserving Routing Techniques
3. Adversary Model
4. Privacy Evaluation Model
5. Security Analysis

1. Attackers Modules:

In this module we form the WSN network area and the appearance of an endangered animal (Attackers) in a monitored area that is survived by wireless sensor, at the each time the inside and outside sensors are sensing to find out the attackers location and the timing. This information is passed to the server for analyzing. After analyzing the commander and Hunter they are also can participate this wireless network. In the commander and hunter itself some intruders are there, our aim to capture the attackers before attempting the network.

2. Privacy-Preserving Routing Techniques:

In this module presents two techniques for privacy preserving routing in sensor networks, a periodic collection method and a source simulation method. The periodic collection method achieves the optimal location privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication cost, and latency; it can be effectively applied to real-time applications. In this paper, we assume that all communication between sensor nodes in the network is protected by pair wise keys so that the contents of all data packets appear random to the Global eavesdropper. This prevents the adversary from correlating different Data packets to trace the real object.

3. Adversary Model:

For the kinds of wireless sensor networks that we envision, we expect highly-motivated and well-funded attackers whose objective is to learn sensitive location-based information. This information can include the location of the events detected by the target sensor network such as the presence of a panda. The Panda- Hunter example application was introduced in, and we will also use it to help describe and motivate our techniques. In this application, a sensor network is deployed to track endangered giant pandas in a bamboo forest. Each panda has an electronic tag that emits a signal that can be detected by the sensors in the network. A clever and motivated poacher could use the communication in the network to help him discover the locations of pandas in the forest more quickly and easily than by traditional tracking techniques. In any case, it should be feasible to monitor the communication patterns and locations of events in a sensor network via global eavesdropping. An attacker with this capability poses a significant threat to location privacy in these networks, and we therefore focus our attention to this type of attacker.

4. Privacy Evaluation Model:

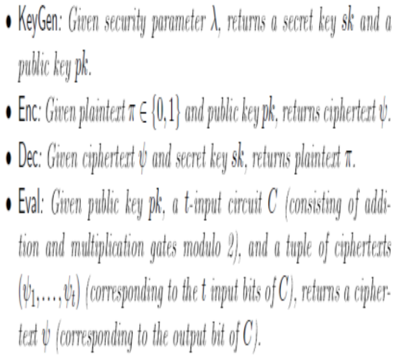
In this module, we formalize the location privacy issues under the global eavesdropper model. In this model, the adversary deploys an attacking network to monitor the sensor activities in the target network. We consider a powerful adversary who can eavesdrop the communication of every Sensor node in the target network. Every sensor node i in the target network is an observation point, which produces an observation (i, t, d) whenever it transmits a packet d in the target network at time t. In this paper, we assume that the attacker only monitors the wireless channel and the contents of any data packet will appear random to him.

5. Security Analysis:

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

V. Algorithms

A. *HOMOMORPHIC ENCRYPTION ALGORITHM:*



- KeyGen: *Given security parameter λ, returns a secret key* sk *and a public key* pk.
- Enc: *Given plaintext $\pi \in \{0,1\}$ and public key* pk, *returns ciphertext ψ.*
- Dec: *Given ciphertext ψ and secret key* sk, *returns plaintext π.*
- Eval: *Given public key* pk, *a t-input circuit C (consisting of addition and multiplication gates modulo 2), and a tuple of ciphertexts $(\psi_1, \ldots, \psi_t)$ (corresponding to the t input bits of C), returns a ciphertext ψ (corresponding to the output bit of C).*

VI. CONCLUSION AND FUTURE WORK

Proposed an efficient privacy preserving and secure data retrieval method using homomorphic encryption technique for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

The future can extends user validation for set of attribute in authentication of multiauthority network environment. We can hide the attribute in access control policy of a user. Different users are allowed to decrypt different pieces of data per the security policy.

REFERENCES

[1] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,”Cryptology Print Archive: Rep. 2010/351, 2010.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proc. ASIACCS, 2010, pp. 261–270.

[3] S. S.M. Chow, “Removing escrow from identity-based encryption,” inProc. PKC, 2009, LNCS 5443, pp. 256–276.

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

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc.ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

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

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

[8] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably secure and efficient bounded ciphertext policy attribute based encryption,” inProc. ASI-ACCS, 2009, pp. 343–352.

[9] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” inProc. ACM Conf. omput. Commun. Security, 2009, pp. 121–130.

[10] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, “P-signa-tures and noninteractive anonymous credentials,” inProc. TCC, 2008, LNCS 4948, pp. 356–374