International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 14, Number 12 (2018), pp. 1079-1085
© Research India Publications
http://www.ripublication.com

Network Security for Emerging Application Using Disruption Tolerant Sensor Network

V.Umesh

Research Scholar Department of Computer Science,
Bharathiar University, Coimbatore, India.

Abstract

Data means collection of intermittently connected nodes. In traditional networks, Intruder nodes within DTSN may try to attempt data destruction in transmits the data to its destination. Disruption-tolerant sensor network (DTSN) technologies are becoming successful solutions that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes by using a prims routing algorithm to find shortest path from source and destination. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data communication. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE DTSN introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. Here the proposed secure data communication using CP-ABE for DTSN where key authorities manage their attributes independently and also demonstrate to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant sensor network for energy efficiency Key words: DTSN, security, encryption, routing

Keywords: DTSN, security, encryption, routing.

I INTRODUCTION.

A sensor network consists of large number of sensor nodes. Each sensor node capable of sensing, data processing, computing, wireless communicating and monitoring object of interest or environmental conditions such as temperature ,sound, embedded processing, humidity, pressure, light intensity. Disruption Tolerant sensor Network (DTSN) has grown to a healthy research topic because of its suitability for challenged environments characterized by heterogeneity, long delay paths and unpredictable link disruptions. DTSN program is an emergent technology that permits access to information when stable end-to-end paths do not exist and communications access cannot be secure. As the technology of DTSN networks matures are used in numerous applications and emerging as an area of active research. Since Sensor node can be deployed in environmental monitoring, medical care, and home appliance management. It can be attacked during data transmission the need for effective security mechanisms. It's is important to provide secure communications between sensor nodes and base stations or Vice versa. Security should be considered because most of sensor possess various mission-critical task hence DTSN network need security.[8] [9] [10][11].

Due to the intermittent connectivity it is very difficult to maintain end-to-end connections. This allows the forwarding of data, only if it is in contact with other nodes. DTSN technology makes use of persistent storage within network nodes, along with the opportunistic use of mobility and aims at solving both challenged networks problems and independent networks incompatibility [1][2][3][4]. Disruption-tolerant sensor network (DTSN) technologies are becoming successful solutions that allow devices to communicate themselves. DTSN have a broad range of potential applications e.g. military battlefields, vehicular communications deep space communications, habitat monitoring, and Internet access in rural areas[5][6].

II . SECURITY GOALS, SCHEME AND STRATAGY

Security goals

The secure for the sensor nodes can be given by the following security goals:

Confidentiality*:* Data must be protected from being captured by any data adversaries.

Authentication*:* Need to know if the messages are from the node it claims to be from, determining the reliability of message's origin

Security Scheme

The security requirements of a wireless sensor network can be classified as follows [12 – 15, 17]:

Data Authentication: Make sure that the data is initiated from the exact source.

Data Confidentiality: Make sure that only authorized sensor nodes can get the

content of the messageThere are two types of techniques used to transfer the data from source to destination

1. Unicast routing
2. Multicast routing

Unicast is the transferring of data from 1 node to other that is from single source to single destination and Multicast routing, which refers to the transmission of the same data to several destinations. Research shows that unicast DTSN has more importance. It reduces the number of packet transmission, optimizes the bandwidth consumption and Save the node energy.

III. UNICASTING IN DTSN

There [1][7] is a need for different methods and techniques for secure path formation. For a secure transmission, broadcasting uses the leaf nodes which are assigned keys based on all forward nodes above them. Secure unicasting scheme considers the benefits of key management techniques; the root to key management is the key distribution centre which uses a logical key. The unicasting system provides a secure communication mechanism to ensure the data security, integrity and verifiability. Moreover, it can be justified against security attacks and known routing attacks. There are various schemes that can be incorporated to form a secure transmission path are through key management techniques or providing security to the layers or to the data that has to be transmitted. unicast is the communication paradigm of one-to one A unicast group can also have one or more senders. unicasting in DTSN evaluates its real impact and comparing. The unicast requirement over DTSN is based on the application nature.

IV. EXISTING SYSTEM

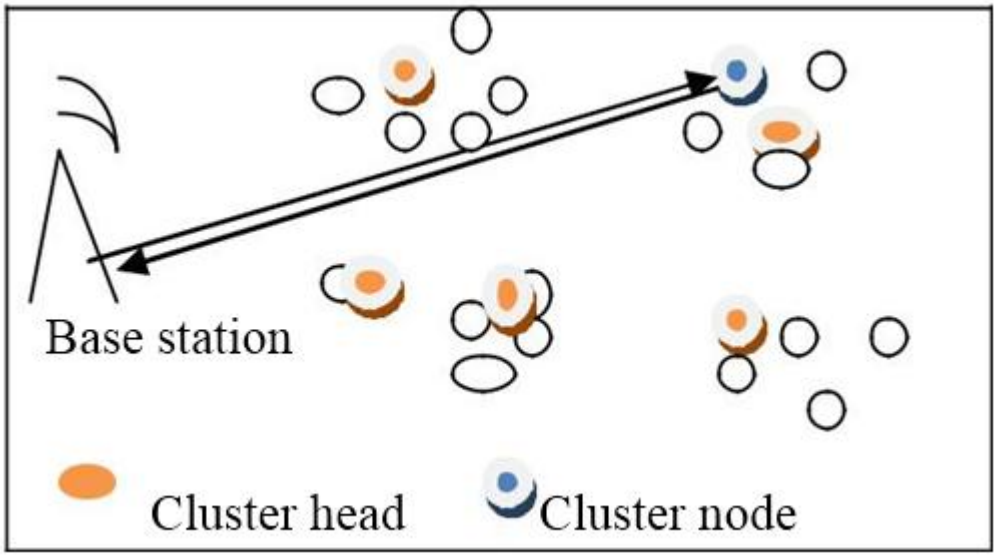
The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data communication in DTSN. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, 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 decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy [2][4].

V. PROPOSED SYATEM

The Propose an attribute-based secure data communication scheme using CP-ABE for communication in DTSN. The proposed scheme features the following achievementFirst, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptions

can define a fine-grained access policy using any monotone access structure 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 DTSN architecture. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

Proposed work aims providing a secure data communication. The scheme involves two steps: first is election of the cluster head in the cluster . Data is sent to from base to destination using the prmis algorithm to fine the shortest path. Second step is the data is sent communication happens using the CP-ABE scheme.



System Architecture

Assumptions:

1. The network considered is cluster based network.
2. All nodes are static in the cluster formation.
3. Node are alive throughout the lifetime and all Nods process minimum resources such energy Criteria, processing speed, storage capacity.

The data communication from base station to Destinations done using the shortest path using the Prims algorithm

Algorithm-1: Prims for finding shortest path prime test n {

```
  set max [expr wide(sqrt(n))]
  if (n%2==0) (return [list 2 [expr n/2]])
  for (set i 3) ($i<=$max) (incr i 2) {
    if (n%i==0)(return [list i [expr n/i]])
  }
  return 1
}
```

VI. ANALYSIS

When the data is sent from base station to destination it uses the prims algorithm to find shortest path and reach thedestination. The CP-ABE scheme is used for secure data communication in network, it produce the public key and private key. In cluster based network ,node 22 is considered as the destination and the data is sent from base station to destination using prims algorithm to find the shortest path ,the path found is 20,27,45,17,35,34, it travels 3 clusters to reach the destination .CP-ABE scheme is used for secure data communication it produces the public key and private key .The energy consumed for public key and private key is 56.56joules and 33.94joules. The average energy required for node and network is 22.62 joules and 24.90 joules. The average node energy, public key, private key differs as per the destination.

Destinations	Intermediates Nodes	Average path Energy	PDR in %
22	42,43,44,18,35,34	22.62joules	151.5
42	20,45,17,35,34	22.64joules	121.2
28	43,44,18,35,34	22.81joules	178.1
7	9,10	22.66joules	84.55

When the simulation is done for different destinations, the trace file is generated to calculate the packet delivery ratio. The awk script is used that is packet.awk, using the packet.awk we can check the packet delivery ratio for different destination , for example in network 22 is the destination the generated packets are 249 the delivered packets are 378 the ratio is 151.83 , for destination 42 the generated packets are 249 the delivered packets are 310 the ratio is 121.55 , for destination 28 the generated packets are 249 the delivered packets are 445, the ratio is 178.98, for destination 7 the generated packets are 249 , the delivered packet is 210 the ratio is 84.55.

VII. CONCLUSION

In DTSN the security is the major task to be provided. DTSN technologies are becoming successful solutions in all applications that 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 secure data communication issues. In the proposed an efficient and secure data communication method using CP-ABE .It also produces the fault tolerating and reduces the packet drop ratio, energy efficiency high

REFERENCES

[1] N.Bhutta,G.Ansa, E. Johnson, N.Bhutta,G.Ansa, E.Johnson Security analysis for Delay/Disruption Tolerant sensor network ",International jornal of research and technology2009

[2] J.Iswariya, Mr.J.Lourdu Xavie "A Secure Communication Model to Detect Flooding Attacks in Disruption Tolerant Networks",International journal of engineering and computer science jan 2014

[3] D.S.Delphin Hepsiba, S.Simla Mercy, S.Prabu, "Secured Data Forwarding Technique in Disruption Tolerant Networks-Survey" International Journal of Advanced Research in Computer and Communication Engineering Feb 2014.

[4] Jingzhe Du, Evangelos Kranakis, "Distributed Key Establishment in Disruption Tolerant Location Based Social Wireless Sensor and Actor Network", International journal of engineering 2013

[5] S.Shanmugasundaram and S.Chitra, " Privacy Preserving and Secure Data Retrieval in Sensor Network using Homomorphic Encryption Algorithm", International Journal of Emerging Technology in Computer Science & Electronics 2015

[6] Peng Yang, Mooi Choo Chuah, "Context-Aware Multicast Routing Scheme for Disruption Tolerant Networks",IEEE 2013

[7] N. Asokan, Kari Kostiainen, Philip Ginzboorg, J¨org Ott2, Cheng Luo2, "Towards Securing Disruption-Tolerant Networking", research center NRC-

TR-2007-007, 2007.

[8] Cheng-Lung Yang, WernhuarTarng, Kuen-Rong Hsieh and Mingteh Chen National Hsinchu University of Education, Hsinchu, Taiwan Ralink Technologies, Hsinchu, Taiwan Micrel Semiconductor Inc., San Jose, California, U.S.AA Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography IEEE 2010.

[9] XiaowangGuo ,Jianyong Zhu Research on Security Issues in Wireless Sensor Networks International Conference on Electronic & Mechanical Engineering and Information Technology IEEE 2011

[10] Abhishek Jain, Kamal Kant M. R. TripathySecurity Solutions for Disruption Tolerant Networks Department of Computer Science & Engineering ASET, Amity University Noida, India IEEE 2012.

[11] T.Thenmozhi, Dr.R.M. Soma sundaram Dean Towards an approach for improved security in Wireless Sensor Networks Department of Sciences SNS College of Engineering Coimbatore, India IEEE 2012