IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Highly Secured Data Encryption In Decentralized Wireless Networks

Amol G Dhoke, Prof P S Kulkarni

[1] Computer Science and Engineering, Gondwana University,
Chandrapur,442401,Maharashtra,India

[2] Information Technology, Gondwana University,
Chandrapur,442401,Maharashtra,India

Abstract

As the use of web side information for critical services has been increased, the significant amount of attacks against Network applications has grown as well. To protecting many Network applications, many of intrusion detection systems have been proposed. Several techniques which are meant for detection of Network application related attacks. The Attacking detection system provides the following: Monitoring and analyzing of user and system activity. Auditing of system an arrangement of parts and vulnerabilities, Evaluating the nature of the integrity of the files and critical system, Activity patterns of relating to the use of statistics analysis , Abnormal activity analysis, Operating system audit.

Keywords: *Side information, Attacking detection, operating system audit.*

1. INTRODUCTION

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. 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. Some of the most challenging issues are the enforcement of authorization policies and the policies update for secure data retrieval. Attribute-based encryption (ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key Management and coordination of attributes issued from different authorities, proposing a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. To apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network data sets in order to illustrate the advantages of using such an approach.

2. PROBLEM DEFINATION

- Military Network should require increased protection of confidential data including access control methods.
- In many cases, it is desirable to provide differentiated access services such that

Data access policies are defined over user attributes or roles, which are managed by the key Management System. It propose a D2C2 algorithm for visual pattern discovery by joint analysis of visual content and side information. A content collection is partitioned into subsets based on side information, and the unique and common visual patterns are discovered with multiple instance learning and clustering steps that analyzes across and within these subsets. Those patterns help to imagine the data content and generate vocabulary-based features for semantic classification. The proposed framework is rather general which can handle all types' offside information, and incorporate different common/unique pattern extraction algorithms. One future work is to improve the generation of common patterns by emphasizing the shared consistencies, instead of the current heuristic clustering.

ISSN 2348 – 7968

3. PROPOSED METHOD

i. Key Authorities: They are key generation centers that generate public/secret parameters for ABE. The key authorities consist of a central authority and multiple local authorities. Assume that there are secured and capable of relied communication channels between a central authority and each local authority during the initial key setup and generation phase.–

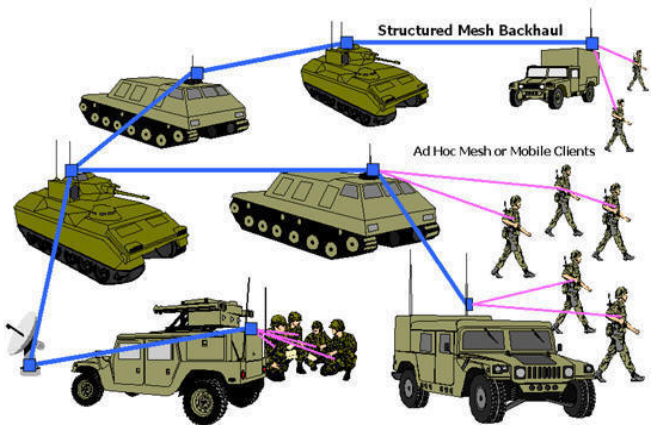

Fig 1 :- Decentralized Military Network

Each local authority manages different attributes and issues corresponding attribute keys to users. They permit differential access rights to individual users based on the user attributes. The key authorities are assumed to be honest but curious. That is, Local authorities will honestly execute the assigned tasks in the system, however users would like to learn information of encrypted data possible.

ii. Storage node: An entity that stores data from senders and provide corresponding access to users. It may be mobile or lacking in movement. Similar to the previous schemes, Assume the storage node to be semi trusted that is honest but curious.

iii. Sender: This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

iv. User: This is a mobile node who wants to access the data stored at

the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not abrogate in any of the attributes, then he will be able to decrypted the International Data Encryption Algorithm i.e IDEA Algorithm and obtain the data. Since the key authorities are half-trusted, they should be deterred from accessing plaint text of the data in the storage node; they should be still able to issue secret keys to users. In order to realize this somewhat in mutually consistent requirement, the enter authority and the local authorities engage in the arithmetic 2 PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. 2 PC protocol prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually.

4. METHODLOGY

Attribute-based secure data retrieval scheme using ABE for decentralized DTNs. The present scheme features the following achievements. First, instant attribute abrogation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-texture access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key management problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key permits protocol generates and gives user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2 PC protocol dissuade the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone.

Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data intent to be private and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

ISSN 2348 – 7968

5. THE TRIPLE DES ALGORITHM

Use of multiple length keys takes us to the Triple-DES algorithm, in which DES is concerned 3 times. Triple DES is simply one more way of DES operation. It takes three 64-bit length of keys, total key length is 192 bits. In Particular Encryption, we simply type in the entire 192-bit (24 character) key comparatively than entering each of the three keys independently. The Triple DES DLL then fragments the user supplied key into three sub keys, filling the keys if wanted so they are each 64 bits long. The method for encryption is totally the similar as regular DES, but it is occured three times. Hence the name Triple DES, The data is encrypted with the first key, then this same encrypted data is decrypted with the second key, and finally this same decrypted data is encrypted again with the third key. Triple DES, also called as 3DES. As a result, Triple DES runs three times comparatively than standard DES, but is highly secure if used correctly.

The method for decrypting data is alike as the method for encryption, other than it is executed in reverse. Same in DES, something is encrypted and decrypted in 64-bit chunks. Lamentably, there are little bit of weak keys that one should be care of it: if all three keys, the first and 2nd keys, or the second and third keys are the matching, then the encryption method is absolutely necessary the identical as standard DES. This condition is to be stay away because it is the alike as using a actually slow version of all time DES.Note that even though the input key for DES is 64 bits in length, the real key used by DES is of 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be placed so that every time an odd number of 1s in every byte. These parity bits are not necessary, so only the seven most important bits of each byte are used, out come in a key length of 56 bits. This means that the successful key uses for Triple DES is really 168 bits because each of the three keys carry 8 parity bits that are not used when in the encryption method.

The Algorithm

Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits (except equal or same bits). The algorithm of Encryption is i.e ciphertext = EK3(DK2(EK1(plaintext))).

I.e., DES encryption with K1, DES decryption with K2, then DES encrypt with K3.

Decryption is the reverse process i.e plaintext=DK1(EK2(DK3(cipher text))). that is decryption with K3, encryption with K2, then decryption with K1.Each an every one triple encryption encrypts one block of 64 bits of data.In every case the middle operation is the backward of the first and last. This enhanced the power of the algorithm during using keying option 2, and supply reverse compatibility with DES with keying option 3.

The Key options

The Levels define three keying options:

I. Keying option 1: All three keys are independent.

II. Keying option 2: K1 and K2 are not identical, and K3 = K1.

III. Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.

Keying option 1 is the strongest, with 3 × 56 = 168 not identical key bits. Keying option 2 gives security, with 2 × 56 = 112 key bits. This option is better than simply DES encrypting two times, e.g. with K1 and K2, because it saves against attacks. Keying option 3 is equals to DES, with only 56 bits of key length. This option provides backward similarity with DES, because the first and second DES operations abandon. It is no prolonged approved by the National Institute of Standards and Technology (NIST),] and is not supported by ISO/IEC 18033-3.

6. IMPLEMENTATION OF ZIGBEE DEVICES

ZigBee is an established set of specifications for wireless personal area networking (WPAN), i.e. digital radio connections between computers and related devices. WPAN small Rate or ZigBee gives identifications for devices that provides small data rates, takes very small power and are thus makes by long battery life. ZigBee will achieve totally networked homes where every devices are able to share and be checked by only one unit. The ZigBee Alliance, the leveled body which defines ZigBee, also produce application profiles that permits multiple OEM vendors to produce exchange and use the products. The recent list of application profiles produced or in the works are:

- Home Automation
- ZigBee Smart Energy
- Telecommunication Applications
- Personal Home

The association between IEEE 802.15.4 and ZigBee is same to that between IEEE 802.11 and the Wi-Fi Alliance. For non-commercial purposes, the ZigBee identification is available free to the general public. An entry standard membership in the ZigBee networks, called Adopter, costs US$ 3500 annually and gives permits to access to the as-yet not published identification and permits to produce products for market using the

ISSN 2348 – 7968

identifications. ZigBee is one of the world standards of networks protocol developed by the applicable task force under the IEEE 802.15 working group. The fourth in the sequence, WPAN small Rate/ZigBee is the new and gives identifications for devices that gives small data rates, takes very small power and are thus characterized by extended battery life. Other level like Bluetooth and IrDA address large data rate applications such as voice,video data and Local Area networks.

ZigBee devices are energetic restrict to a through rate of 250Kbps, compare with Bluetooth's much huge pipeline of 1Mb/s works on the 2.4 GHz ISM band, which is obtained throughout most of the global .In the market, ZigBee is being showed for everything from associating small-power home devices such as smoke alarms, light controls. The identified large range of operation for ZigBee devices is 250 feet (76m), considerable further as compared to that used by Bluetooth capable devices, even though security related to increased over "sniping" Bluetooth devices remotely, may gives to hold real for ZigBee devices as well. Because of its small power output, ZigBee devices can survive themselves on a low battery for many months, or even years, making them perfect for install-and-forget tasks, such as small household systems. Prophecy of ZigBee installation in future, many of based on the volatile use of ZigBee in automated house equipment tasks in China, look to a near future during upwards of sixty ZigBee devices may be searched in an middle size American home, all communicating between other freely and managing common tasks that not seamless.

Fig 2:- Zigbee Device

7. ZIGBEE CHARACTERISTICS

The focus of network applications under the IEEE 802.15.4 ZigBee leveled contains the characteristics of small energy consumption, necessary for only two big modes (Tx/Rx or Sleep),huge solidity of nodes per network, small costs and simple execution. These Quality are enabled by the following features,

• 2.4GHz and 868/915 MHz dual PHY techniques. This to be entitled three license-free bands: 2.4-2.4835 GHz, 868-870 MegaHz and 902-928 MHz. The amount of channels specified to every frequency band is specified at sixteen (numbered 11-26), one (numbered 0) and ten (numbered 1-10) respectively. The large frequency band is relevant worldwide, and the small band in the areas of North America, Europe, Australia and New Zealand .
• Low power consumption, with battery life extends from months to years. Taking everything into account the amount of devices with remotes in use at recent, it is not difficult to see that more amount of batteries want to be provides each so often, needs well ordered , repeating expenditure. In the ZigBee level, lengthy battery life is gets by either of two means: uninterrupted extension network connection andnot fast but sure battery decreases , or irregular connection and even slower battery drain.
• Large data rates permits for every of these frequency bands are specified as 250 kbps @2.4 GHz, 40 kbps @ 915 MHz, and 20 kbps @868 MHz.
• Large throughput and small latency for small duty cycle applications (<0.1%)
• Channel entries utilizing Carrier Sense Multiple Access with Collision Avoidance (CSMA - CA)
• Addressing area of up to 64 bit IEEE address devices, 65,535 networks 50 meter typical covered range.
• Fully reliable “hand-shaked” data transfer protocol.
• Different topologies as shown below: star topology, peer-to-peer, mesh topology.

8. ARCHITECTURE

ZigBee is a home-area network designed specifically to replace the proliferation of individual remote controls and also ZigBee was designed to meet the expectations of the market's need for a cost-effectual, standards-based wireless network that hold up low data rates, small power consumption, security, protection and reliability. To address this requirement, the ZigBee Alliance, an industry working group (www.zigbee.org), is growing standardized application software on top of the IEEE 802.15.4 wireless standard. The alliance is going nearly with the IEEE to make sure an united, total, and interoperable network for the market. For example, the working group will supply interoperability certification testing of 802.15.4 systems that incorporate the ZigBee software layer. The ZigBee Alliance will also distribute as the official trial(test) and certification group for ZigBee devices. ZigBee is the only level-based technology that inscript the requirements of most remote observing and control and sensory network applications. It may be useful to beleive of IEEE 802.15.4 is the physical radio and Device like ZigBee is the objective network and implementation software. Coming after of the standard

ISSN 2348 – 7968

Open Systems Interconnection (OSI) reference model, ZigBee's protocol stack is constructed in layers. The first two layers, physical (PHY) and media access (MAC).

The layers at top of them are defined by the ZigBee Alliance. The IEEE working group progressed the first draft of PHY,MAC in 2003. ZigBee-amenable products works in unlicensed bands worldwide, including 2.4GHz (International), 902 to 928MegaHz (USA), and 868MegaHz (UK). Raw data throughput rates of 250Kb/s can be gain at 2.4GHz (sixteen channels), 40Kb/s at 915MegaHz (Ten channels), and 20Kb/s at 868MegaHz (1 channel). The transmission distance is expected to range from 10 to 75m, rely on power output and environmental features. Like Wi-Fi, Zigbee utilize direct-successions spread spectrum in the 2.4GHz band, with balance-quadrature phase-carrying keying modulation. Channel spread is 2 Mega Hz with 5 Mega Hz channel spacing. The 868 Mega HZ and 900 Mega Hz bands also use straight-successions spread spectrum but with binary phase carrying keying modulation.

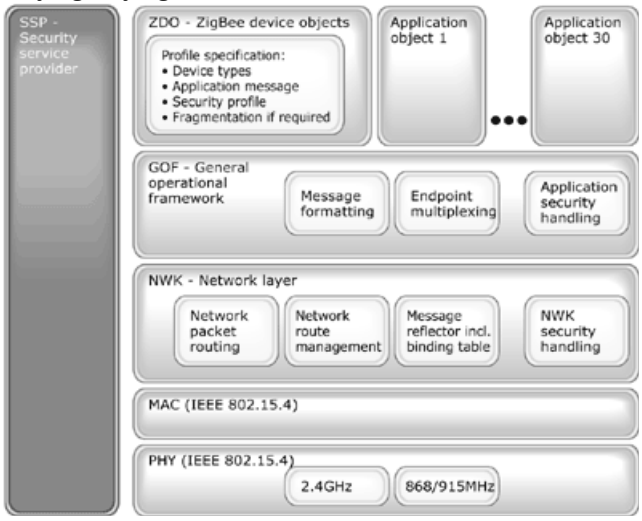

Fig 3:-Zigbee Stack Architecture

9. DEVICE TYPES

These devices own 64-bit length of IEEE addresses, accompanied by option to authorize shorter addresses to decrease packet length, and work in either of two addressing modes – star and peer-to-peer. ZigBee networks utilize 3 device category:

• The *network coordinator* keeps mostly complete network knowledge. It's the most worldly of the three types and needs the most memory and computing energy.

• The *full function device* (FFD) bears all the 802.15.4 functions and characteristics described by the standard. It can use as a network coordinator. Further memory and computing energy create it most suitable for network router functions or it could be utilized in network-edge devices (where the network meets the real world).

• The reduced function device (RFD) supports limited (as described by the standard) functionality to small cost and difficulty. It's usually discovered under network-fringe devices.

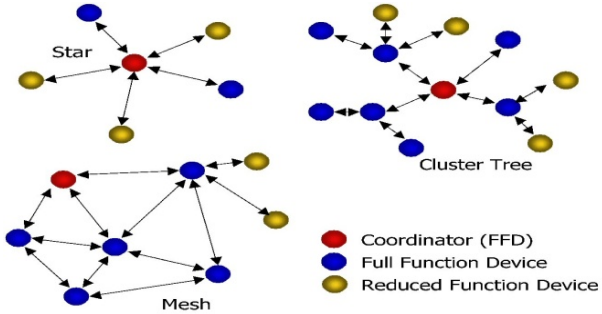

Fig 4 :- Zigbee Topologies

10.Communications Between Nodes

The data being send from sender to receiver is being encrypted using IDEA (International Data Encryption Algorithm).The Zigbee from the sender side is called as co-coordinator and the receiver zigbee is called as Router. The sender computer first encrypts the data using 256 bit key of length, then this encrypted data is being send using coordinator zigbee (sender side) to the receiver(router zigbee),the data is received is then being decrypted using 256 bit key .Because zigbee provides its own mesh networks,all nodes are movable.This helps the soldiers to communicates securely with each others.

The zigbee can create its own mesh networks using low consumption of power.So even there is heavy rainfall or even heavy storm or heavy winds then also the soldiers are able to communicate with each others.The soldier sends a data in voice form will first get encrypted then this encrypted file is send to server called as storage node, from storage node this data will be received by another soldier.The data is highly secured using the IDEA and thus the key changes from time to time,the zigbee which creates its own mesh networks are unable to detect for the attacker.

11. SECURITY

Security and data integrity are important advantages of the ZigBee technology. Tis technology grips

ISSN 2348 – 7968

the security model of the level of IEEE 802.15.4 of MAC sub layer which describes four security features:

• Control of access which the device sustain a list of reliable devices under the network.

• Encryption of data, which utilizes same key 128-bit of length advanced encryption standard.

• Frame unity to secure data from being changed by attackers without cryptographic keys.

•Forming freshness to unaccepted data frames that have been repeated—Controller of network differentiate the freshness significance value with the last known significance value from the device and unaccepted it if the freshness value has not been updated to a new worth value .The real security execution is described by the implementer utilizing a standardized level of toolbox of ZigBee security software.

12. CONCULSION

Technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. It is a scalable cryptographic solution to the access control and secure data retrieval issues. An efficient and secured data obtaining method using this method for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key bond or deed 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.

Acknowledgment

This work was supported by Prop S. Kulkarni, Head, Department of Information Technology**,** R.C.E.R.T, Chandrapur. Prof.Rahila Sheikh, Assistant Professor, Computer Technology, R.C.E.R.T., Chandrapur and Prof. R K.Krishna, Assistant Professor, Department of Electronics, R.C.E.R.T. for their encouragement to accomplish my work on time and also Prof. Nitin J. Janwe, Head, Department of Computer Technology, R.C.E.R.T., Chandrapur and honorable Dr. K. R. Dixit, Principal, R.C.E.R.T., Chandrapur, for being a constant source of inspiration. The authors would like to thank the anonymous reviewers for their valuable and constructive comments on improving the paper.

REFERENCES

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

[2] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in *Proc. IEEE MILCOM, 2006, pp.*1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, “Message ferry route design for sparse ad hoc networks with mobile nodes,” in *Proc. ACM MobiHoc, 2006, pp. 37–48.*

[4] S. Roy andM. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,“Plutus: Scalable secure file sharing on untrusted storage,” in *Proc. Conf. File Storage Technol., 2003, pp. 29–42.*

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated ciphertext-policy attribute-based encryption and its application,”in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[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 n vehicular ad hoc networks,” *Ad Hoc Netw.*, vol. 7, no. 8,pp. 1526–1535, 2009.

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

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

[12] 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.