International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 327-336
http://dx.doi.org/10.14257/ijsia.2015.9.4.30

Applying a Security Architecture with Key Management Framework to the Delay/Disruption Tolerant Networks

Gideon Rajan and Gihwan Cho*

Division of Computer Science and Engineering, Chonbuk National University
567 Baekje-daero, Deokjin-gu
Jeonju, Jeollabuk-do 561-756, Republic of Korea
E-mail: pepsigidy@gmail.com, ghcho@chonbuk.ac.kr

Abstract

Recently, one of the growing hot topics in the field of wireless network is to enable of Delay/Disruption Tolerant Networking (DTN). It aims to solve the long delay paths and unpredictable link disruptions that occur in the challenged networks. In order to maintain a safe and secure DTN model, a secure way of key distribution would be required to provide robustness from all the attacks it suffers. This paper proposes a clear and illustrative security architecture for DTN with secure key management framework to distribute the cryptographic keys to the constituted nodes in a secure way. The performance of how the cryptographic keys work and perform during a node is departed away from the network are discussed. The distributed keys use the public key cryptography to mitigate during the network attacks. Along with the key management protocol, some degree of security features can be achieved with the bundle of security protocol to rescue the network model from any attacks.

Keywords: *DTN, Network Model, Security, Key Management*

1. Introduction

For the past few years, Delay and Disruption Tolerant Networking (DTN) has grown into a healthy topic in the field of networking technology. Many works have been done by the network designers and researches on DTN due to its intrinsic nature of the network. Even though researches on DTN started a decade ago, the principles, architecture and protocols have just been made concrete recently.

It is a quite difficult task to communicate between the nodes located in the exotic places and/or remote areas. Networks like these are usually independent and very difficult to connect with the Internet due to the heterogeneity; these networks are called as the challenged networks or intermittent networks. These networks are usually deployed in the exotic places such as the deep space, deep underwater, war zones, environmental and disaster areas. They pose the difficulties in sending data to long distances due to the long delay and link disruptions. Intermittently Connected Networks (ICN) concept has been proposed to overcome the difficulties; nodes are capable of communicating with each other even if the end-to-end connectivity is unavailable. Due to the lack of continuous end-to-end connectivity, ICN fails to complete the deficiency of the challenged networks. DTN is the special networking architecture which resolves the problem both in the challenged networks as well as the independent networks.

DTN offers an application interface structured around a reliable store and forward packet exchange, with restricted or null expectations of end-to-end connectivity. RFC 4838 defines DTN as a generalized store and forward network overlay [1, 2]. The DTN

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

architecture was designed not only to accommodate network connection disruptions, but also to provide a framework for dealing with lower layers heterogeneity by introducing a new layer called “bundle layer”. The protocol used in bundle layer is called bundle protocol, and the nodes that rely on bundle protocol are called as bundle nodes. Bundle nodes placed in exotic locations collects the data, bundle it and store inside its memory for a long period. They do not follow any topology because the nodes are mobile in nature; for example, bundle nodes are deployed under the ocean to collect the oceanographic environment data, where the nodes will be drifted off by the current of the ocean. Once the bundle node gets contact with any neighbor node in the network, it transmits all the data to its neighbor.

Like the other networks, DTN should be provided with a perfect security procedure or architecture to maintain the network from any threats. Cryptographic keys play a vital role in transferring the messages securely from one node to other node. This paper deals with the DTN security architecture along with the cryptographic key distribution through the network. Due to the nature of the DTN, it is a difficult job to collect all the data from the bundle nodes securely. The cryptographic keys are transferred to all the nodes in the network and it retrieves all the data from the nodes securely. The performance of how the cryptographic keys work is discussed with two cases and how it will perform during a node is departed away from the network. The distributed keys in the bundle nodes use the public key cryptography to mitigate during the network attacks. All the nodes use the four security blocks of the Bundle Security Protocol to secure the network.

The rest of the paper is organized as follows. Section II is about the previously related works. Section III discusses about the threats and the Bundle Security Protocol. Section IV proposes the network model and a secure key distribution process. Section V discusses the key and security performance in DTN. Section VI concludes the paper.

2. Related Works

Many Researches have been propose for the security and the key management techniques for the DTN architectures, but still it is far behind from using it practically. Reference [3] proposed a DTN security architecture which discusses about the store and forward style of communication. It supports hop-by-hop and end-to-end authentication to ensure data correctness before forwarding using bundle authentication block. It focuses on different key management parameters based on proxy certificates and Public Key Infrastructure (PKI).

The security mechanism for the interactive satellite remote education system is proposed by making use of a conditional access module based on user intelligent card for broadcast server and satellite terminal nodes [4]. The USB key is used as the storage device hardware which ensures that the private key won’t be appear or store temporarily, so it will prevent the illegal users from capturing the private key. Reference [5] proposed a security analysis and bundle protocol specification for DTN space-based networks.

Our work provides a cryptographic key management of securing the message transferring from one node to the others. It aims to provide to be a better way of securing the messages from the attacks. Unlike other works, our method provides the security of the nodes even during the nodes is away from the network.

3. DTN Security Architecture

3.1. Threats

Every network is posed under the threat to attacks; likewise DTN suffers from threats such as passive and active attacks. The passive attacks are the major concern due to the broadcast of the internet everywhere. In a passive attack, an intruder may extract some sensitive data just by monitoring the broadcast of a satellite. The intruders might eavesdrop on either intended or non–intended data. They might have an aim of monitoring the traffic for gaining knowledge or obtain information on private parties.

Active threats are more difficult to implement than passive threats since they require more sophisticated resources to carry on the attack. Some examples are (a) tampering messages, which deals with the modification of any confidential messages of the third parties. The attacker steals and reads the original message and tampers it with the duplicate message. (b) replay attacks, where the intruder sends the already sent old messages to confuse the receiver. (c) masquerading, the intruder gains access to be an authorized user and could steal/tamper any confidential messages. (d) Denial of Service (DoS), in which the main goal of the intruder is to exhaust the network and prevent the authorized user from accessing the network.

3.2. Security Protocol

Conventional security protocols do not perform well in the case of high link disruptions and long delays. Thus a new security protocol is introduced for the DTN requirements called the Bundle Security Protocol (BSP). The progress on the BSP are still been working and the main features of the protocol are defined in the RFC 6257. There are three main aspects; firstly it is to identify the difference between the bundle nodes that supports the BSP and the nodes that does not support them. The bundle nodes that do not support the BSP will be transparent. Secondly, BSP supports both hop-by-hop and end-to-end authentication valid before forwarding. Thirdly, the bundle payload and the bundle data (*e.g.*, metadata) can be protected by different passwords.

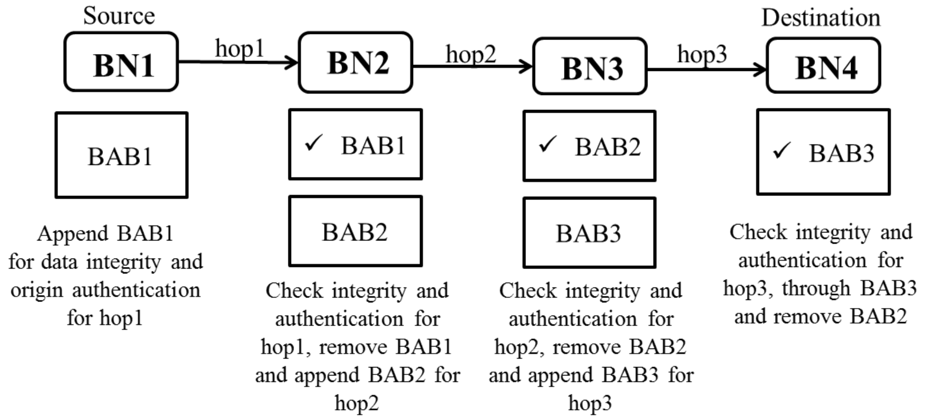
Source
Destination
BN1
hop1
BN2
hop2
BN3
hop3
BN4
BAB1
✓ BAB1
BAB2
✓ BAB2
BAB3
✓ BAB3
Append BAB1 for data integrity and origin authentication for hop1
Check integrity and authentication for hop1, remove BAB1 and append BAB2 for hop2
Check integrity and authentication for hop2, remove BAB2 and append BAB3 for hop3
Check integrity and authentication for hop3, through BAB3 and remove BAB2

Figure 1. BAB for hop-to-hop Security Check

BSP of the DTN security requires that before forwarding any bundle it must be authenticated and integrity checked. To implement the security in BSP, the following four security blocks are added as

- Bundle authentication block (BAB)
- Payload integrity block (PIB)
- Payload confidentiality block (PCB)
- Extension security block (ESB)

Figure 1 shows how BAB is used to assure the authentication and the integrity of every bundle when it travels through every hop-by-hop. BAB that is provided at every BSP provides bundle to check whether the bundle is authenticated. Figure 2 shows how PIB is used to check the authentication and the integrity for multiple hops, usually between end-to-end or consecutive nodes. The PIB may be verified by any node to find the PIB-source but does not need to check with the PIB-destination because the key needs to verify the PIB authenticator will be the public key associated with the PIB-source [7].

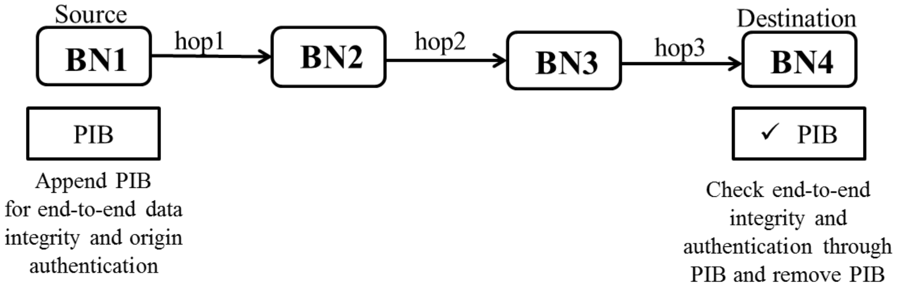
Source
BN1
hop1
BN2
hop2
BN3
hop3
Destination
BN4
PIB
Append PIB for end-to-end data integrity and origin authentication
✓ PIB
Check end-to-end integrity and authentication through PIB and remove PIB

Figure 2. PIB for end-to-end Security Check

While PCB provides the confidentiality of the every block that is transferred from end-to-end, ESB provides the protection for the non-payload related portion of a bundle. The ESB provides the confidentiality and integrity for all the blocks, especially the metadata of the bundle. Its block protection is not transparent, so it is very difficult to access. The ESB keys are very different from the other security blocks, that they can get access to any selected intermediate nodes, for example routers, without compromising the end-to-end security.

4. The Proposed Key Management Framework

Owing to the DTN requirements for long delays and link disruptions, new security architecture with the securable key management is proposed. The DTN architecture is provided with all the security features of the BSP. The key management plays a vital role in distributing the cryptographic keys securely throughout the network.

4.1. Network Architectural Model

Figure 3 shows the proposed network architectural model for the DTN. It consists of a broadcast server which is considered as a base station to collect all the data from the bundle nodes. Let us assume that the broadcast server and the Key Distribution Center (KDC) both are located within the same organization. The broadcast server is followed by the DTN Gateway Node. The Gateway node acts as the gateway for the data passing from broadcast server to all over the network. It is followed by the Intermediate Nodes. Intermediate node acts as the connecting point between all the bundle nodes and the gateway nodes. The intermediate node plays a crucial role in collecting all the sensed data forwarded from the bundle nodes. The intermediate node has the large storage capacity and computational power to store all the data received from the bundle nodes. In space DTN, the intermediate node acts as the satellite orbiting around the planet and bundle nodes can be a probe or rover in the landscape of the planet. The bundle nodes collect the data of its surrounding and send the data back to the intermediate node. Sometimes, the bundle node tends to move away from the transmission range of the intermediate node which may lead to the link disruption.

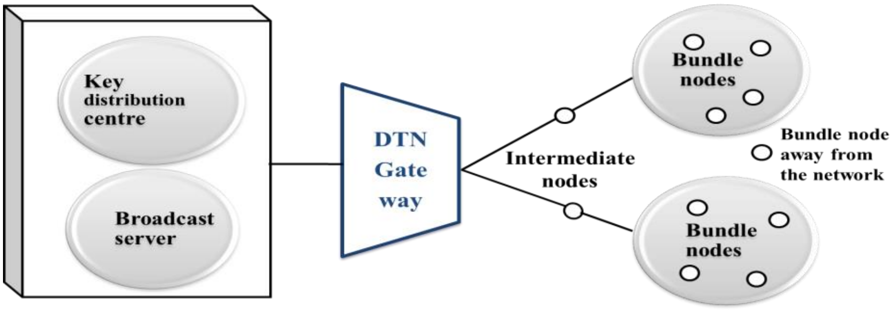

Figure 3. The Proposed DTN Network Model

4.2. Key Management

Securing of the DTN network model begins with the secure key management process. Every node in the network exchange and store the keys for the communication and the transmission of data between each other. Initially, all the nodes in the network have their own unique ID and the shared personal key. Base station plays an important part in collecting and distributing all the keys throughout the network. The KDC that is located with the base station has a large pool of seeds that are provided on request from the base station. The KDC provides n number of seeds to the base station to derive keys for the nodes on the network. A seed can be defined as an entity through which a node can derive keys [6, 8]. It can be subdivided into many keys for various purposes. Different kinds of networks may have different kinds of seeds.

4.3. Key Distribution

Initially during the installation of the network, base station collects a seed from the KDC to derive n number of public and private keys for all the nodes in the network. The derived public and private keys are distributed to the nodes all over the networks and they are used for encryption and decryption of all the messages in every node. Our model proposes the public key cryptography for the safe and secure key distribution. Note that the public and private keys used for encryption and decryption used in this work is denoted by K_P. During the key distribution, the base station collects a seed from the KDC and derives an administration key and a session key using the seed. It encrypts the administration and session keys into message using the shared personal key. The encrypted message is forwarded to the gateway node that has the keys and a seed. The gateway node collects the message and decrypts the message sent from the base station using the shared personal key.

Table 1. Symbols for Keys Distribution

Symbols	Description
K_p	Personal key
$Seed_n$	Seeds used throughout the network
K_{BS-AD}	Admin key of base station
K_{BSS}	Session key of base station
K_{G-AD}	Admin key of DTN gateway
K_{GS}	Session key of DTN gateway
K_{I-AD}	Admin key of intermediate node
K_{IS}	Session key of intermediate node
K_{D-AD}	Admin key of bundle node
K_{DTS}	Session key of bundle node

The gateway node again derives a new pair of keys using the seed provided by the base station. Likewise, the gateway node encrypts a new message and sends it to the intermediate node. The intermediate node again follows the same steps as described above and send it forward to the bundle nodes. Once the bundle nodes receive the keys and the seed from the intermediate node, it derives new keys for sending the collected data. The administration key is used to derive the keys from a seed, the session keys are used to communicate between the each and every node and the seeds are used to derive a new set of keys for every node in the network. The steps of the key distribution from the base station to the bundle nodes of the proposed network are detailed below.

Step1: The seed$_j$ is collected from the KDC seed pool in the base station. The collected seed is used to derive two keys namely the administration key $K_{BS\text{-}AD}$ and the session key K_{BSS}. These two keys along with the seed$_j$ are encrypted with the public key of base station and forwarded to the next node, gateway node.

$$\text{Broadcast Server} \rightarrow \text{DTN Gateway: } (K_P\,[K_{BS\text{-}AD}, K_{BSS}, \text{Seed}_j])$$

Step2: The message received from base station gets decrypted using the private key of the gateway node, which now has the keys and the seed$_j$. The collected seed is used to derive two keys namely, the administration key $K_{G\text{-}AD}$ and the session key K_{GS}. The derived keys along with a seed$_k$ are encrypted using the shared personal key and forwarded to the next node, intermediate node.

$$\text{DTN Gateway} \rightarrow \text{Intermediate node: } (K_P\,[K_{G\text{-}AD}, K_{GS}, \text{Seed}_k])$$

Step3: Similarly, the received message from gateway node is decrypted in the intermediate node which has the seed$_{k}^{.}$ The collected seed is used to derive further two keys namely, the administration key $K_{I\text{-}AD}$ and the session key K_{IS}. The derived keys are then encrypted with the shared personal keys along with a seed$_l$ and forwarded to the next node, bundle nodes.

$$\text{Intermediate node} \rightarrow \text{Bundle node: } (K_P\,[K_{I\text{-}AD}, K_{IS}, \text{Seed}_l])$$

Step4: The keys and seed$_l$ received from the intermediate node are decrypted at the bundle nodes. Bundle nodes again derives two keys namely the administration key $K_{D\text{-}AD}$ and the sessions key K_{DTS} from the seed$_l$ and store the keys for the future use of forwarding the sensed data to the intermediate nodes.

$$\text{Bundle node: } [K_{D\text{-}AD}, K_{DTS}]$$

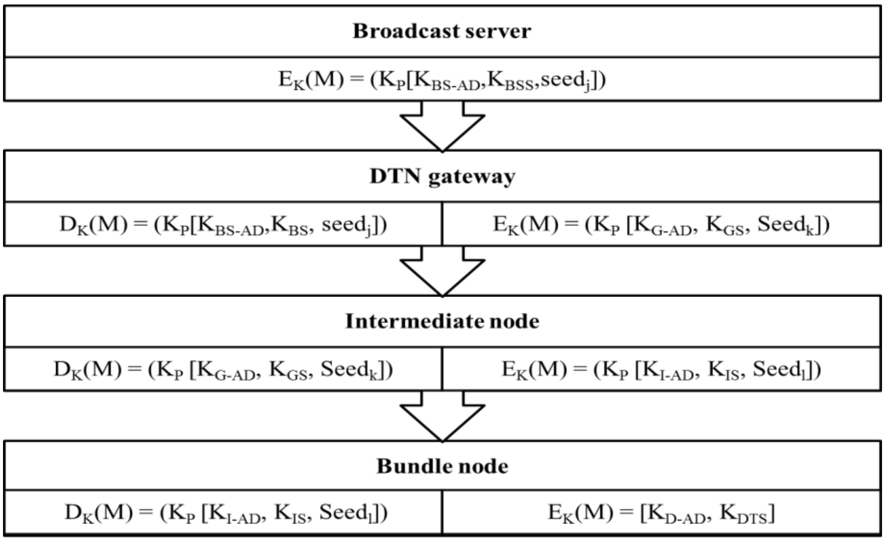
Broadcast server
$E_K(M) = (K_P[K_{BS\text{-}AD}, K_{BSS}, \text{seed}_j])$
DTN gateway
$D_K(M) = (K_P[K_{BS\text{-}AD}, K_{BS}, \text{seed}_j])$
$E_K(M) = (K_P\,[K_{G\text{-}AD}, K_{GS}, \text{Seed}_k])$
Intermediate node
$D_K(M) = (K_P\,[K_{G\text{-}AD}, K_{GS}, \text{Seed}_k])$
$E_K(M) = (K_P\,[K_{I\text{-}AD}, K_{IS}, \text{Seed}_l])$
Bundle node
$D_K(M) = (K_P\,[K_{I\text{-}AD}, K_{IS}, \text{Seed}_l])$
$E_K(M) = [K_{D\text{-}AD}, K_{DTS}]$

Figure 4. Encryption and Decryption of Control Messages

4.4. Encryption and Decryption

The encryption and decryption process proposed in this network model follows a similar pattern in four different nodes of the network. Figure 4 shows the encryption of the control messages starts with the base station where the message consists of keys and seed which are encrypted and proceeds to the next node, gateway node. The gateway node decrypts the message and derives new set of keys, encrypts it into a new message and forwards them to the intermediate node. Likewise the encryption and decryption process goes on till the message of the keys reaches the bundle nodes. Bundle node that has already stored the collected data will now readily transmit once it receives the encrypted message.

As shown in the Figure 5, the bundle node uses the session key to forward the data towards the intermediate node. The intermediate node which collected the entire data sent by the bundle nodes will use the session key to forward the data to gateway node. Likewise all the nodes use session keys to forward the data till it reaches the base station. Base station acts as the bank for collecting all the data forwarded by the bundle nodes.

5. Discussion

The DTN is placed under exotic conditions on the deep space or deep oceans, so the real-time aspects of the key management should be improvised. To ensure the security, all the security services like confidentiality, integrity, non-repudiation are required to provide an end-to-end and hop-to-hop check within the DTN infrastructure [9]. For all the forwarding bundles the DTN security should provide the authentication and integrity checked. Consider that the BSP in all the DTN nodes have an access to the authentication of each other's public key, that is, every DTN node supposed to know the other DTN nodes to whom they are connected.

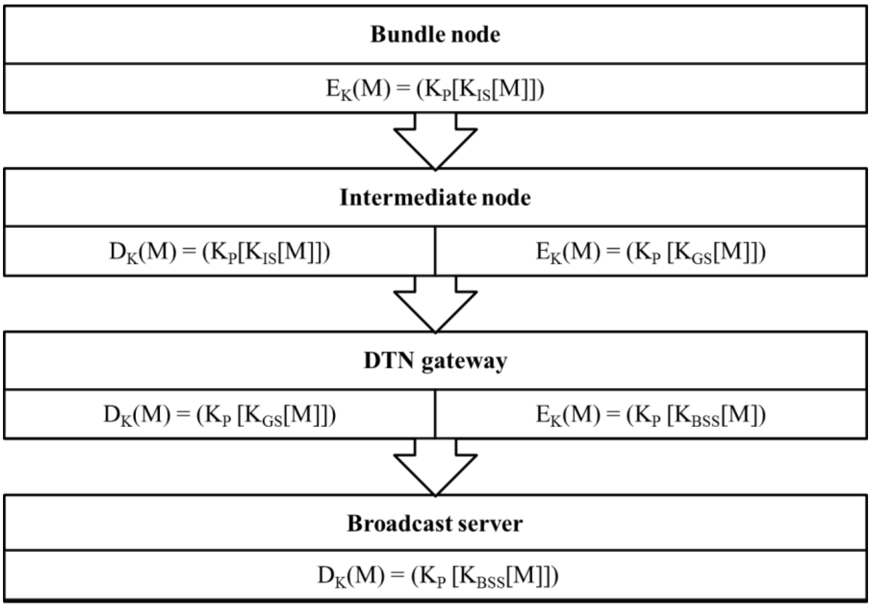
Bundle node
$E_K(M) = (K_P[K_{IS}[M]])$
Intermediate node
$D_K(M) = (K_P[K_{IS}[M]])$
$E_K(M) = (K_P [K_{GS}[M]])$
DTN gateway
$D_K(M) = (K_P [K_{GS}[M]])$
$E_K(M) = (K_P [K_{BSS}[M]])$
Broadcast server
$D_K(M) = (K_P [K_{BSS}[M]])$

Figure 5. Encryption and Decryption of Data Messages

5.1. Intermittent Nodes

The intermediate node which collects all the data provided by the bundle nodes will be far away from the network. So communication between the bundle nodes and intermediate node will be a tedious process. Space and ocean DTN suffers terrible link disruption due to the bundle nodes which travels far away from the network. Our method securely transfers the keys between the networks. Consider that the administration key $K_{D\text{-}AD}$ and session key K_{DTS} with the $seed_l$ is transmitted from the intermediate to a particular bundle node.

The job of the bundle nodes is to collect the data and transmit them to the intermediate node. If the bundle nodes have the necessity to transmit enough data to the intermediate node it will use the session key to transmit the data to the nearest node; which could be either a neighbor bundle node or intermediate node. If the bundle node is not in a hurry or does not have sufficient data to transfer, it will store the received keys and seed inside its memory for a maximum amount of time possible until it could transmit the collected data.

The bundle nodes have the ability to move away from the transmission range or the coverage of the network for collecting the data. Once the bundle node is ready, it transmits all the collected data to the intermediate node or any encountered neighbor bundle node using the session key K_{DTS}. If the bundle node does not have any administration or the session keys due to the reason such as bundle node left the transmission range before the key distribution, it has the ability to bundle the collected data and store them inside its memory for a long time. Once the node enters into the transmission range, the intermediate node will check for the newly possible node. It checks with all the confidentiality and integrity of the node whether it belongs to the network, if positive, the intermediate node will distribute a set of keys and the seed to the newly, available node. Now the bundle node will transmit all the data collected in its memory to the respective intermediate node.

There are some special cases as;

Case 1: when the bundle node moves far away from the network and gets in contact with a neighbor node of other DTN networks from where it is deployed. Consider that the bundle node contains the seed and the keys stored from the previous network; once it encounters any nodes from other networks, it transmits the messages using the old keys. If the neighboring node is from the different network and has a different set of keys, it will reject the data transfer happening between the bundle nodes. The neighboring bundle node will report the newly encountered node in the network to the intermediate node. The intermediate node verifies the newly encountered node and then checks its authentication, confidentiality and integrity and if the new node has the possibility to succeed in the network, the intermediate node derives a new set of administration and session key along with the seed for the newly encountered bundle node. Using the new keys the bundle node will transmit all the collected data to the source through intermediate node.

Case 2: Bundle node uses session keys for transmitting the message to the intermediate node or neighboring node. Note that the session keys acts only for a particular amount of time and once the time period expires, the session key is no longer useful for the bundle node to transmit the message. In cases like this, once the session key gets expired in any bundle node, the bundle node uses the administration key and the seed to derive a new pair of keys. Using the newly derived session key the bundle node will transmit the entire message to the respective nodes.

5.2. Attack Prevention

Like any other networks, DTN network is also vulnerable to all kinds of threats. Our proposed system makes use of the public key cryptography to prevent certain attacks happening on the bundle nodes. The attacker needs to possess a sophisticated way to carry out their attack in any bundle nodes. In the public key cryptography, the bundle node uses the personal private key for the decryption of the messages that the attacker cannot access the messages. The network model will periodically change its public and private keys of every node in the network. The messages are intended to open only by the node that has the particular ID and the key to be open.

Some kind of active attack can be mitigated using the key distribution. Consider that there is an administration key and a session key along with a seed inside a bundle node. The attackers' purpose is to steal the session key that is used for transmitting the messages. Once the bundle node detects the node is being attacked, the bundle node uses the seed and the administration key to derive a new set of session key. Suppose, if a node is compromised, the neighboring nodes will have the ability to detect the attacks and report it to the intermediate node. The intermediate node checks the confidentiality and integrity of the node to determine if it is compromised. Once the intermediate node finds out that the node is being compromised it tries to send a new set of keys to defend the attack.

The BSP has the ability to tackle some of the security threats with the security block. The BSP mainly uses BAB, PIB and PCB for the confidentiality and integrity check to mitigate the attack. In attacks like masquerade, the BSP uses the BAB block for the authentication of the nodes. If there is any attempt sent through the bundles by the attacker who pretends to be an authorized user will be easily checked by the BAB security block. For the denial of service attacks, the bundles will fail to be verified by the BAB security blocks. Some attacks appear as a large number of unauthorized bundles to exhaust the memory. For these kinds of attacks, a light weight mitigation method is used like the cookie techniques. In tampering and eavesdropping attacks, the attacker will listen or modify the bundle payload. These types of attacks can be mitigated by checking the PIB and PCB security blocks. Thus these kinds of serious threats could be taken care of with perfect security models.

6. Conclusions

The proposed DTN security architecture provides a basement of key distribution and prevention of nodes during threats/attacks. One of the key features is its public key encryption/decryption which ensures the security of data transfer. The seeds which are provided by the KDC are the main entities which play the important role in deriving the administration and session keys for all the nodes in the network. The salient feature of the seeds is their ability to provide keys for communication even during the node is link disrupted or away from the network. The cryptographic keys also play a vital role in mitigating the attacks during the key distribution. The BSB uses the security blocks for preventing the different kinds of attack thus keeping the network safe. This work will be a next step further into the future development of secure data transmission in DTN networks.

Acknowledgement

"This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2014065816)"

References

[1] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture" RFC 4838 (2007) Nov., pp. 1-35.

[2] K. Fall and S. Farrell, "DTN: An Architectural Retrospective" IEEE Journal on Selected Areas in Communications, (2008) June, vol. 26, Issue 5, pp. 828-836.

[3] N. Bhutta, G. Ansa, E. Johnson, N. Ahmad, M. AlSiyabi. M, and H. S. Cruickshank, "Security Analysis for Delay/Disruption Tolerant Satellite and Sensor Networks" International Workshop on Satellite and Space Communications (2009) Sept., pp. 385-389.

[4] X. Y. Bai and Y. Huang, "Security Mechanism for the Interactive Satellite Remote Education System which based on DTN" International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (2013) Oct., pp. 46-52.

[5] W. D. Ivancic, “Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks” Aerospace Conference (2010) Mar., pp. 1-12.

[6] S. Hosen, Gideon, G. Cho, “A Robust Key Management Scheme based on Node Hierarchy for Wireless Sensor Networks” International Conference on Computational Science and Its Applications, (2014) June, Vol. 8580, pp. 315-329.

[7] C. Caini and V. Fiore, “Moon to Earth DTN Communication through Lunar Relay Satellites” Advanced Satellite Multimedia Systems Conference and Signal Processing for Space Communications Workshop (2012) Sept., pp. 89-95.

[8] Gideon and G. Cho, “A Securable Key Management Scheme for Delay/disruption Tolerant Networks” International Symposium on Information Technology Convergence (2014) Oct., pp. 180-182.

[9] C. Caini, R. Firrincieli, H. Cruickshank, and M. Marchese, “Satellite Communications: from PEPs to DTN” Advanced Satellite Multimedia Systems Conference and Signal Processing for Space Communications Workshop (2010) Sept., pp. 62-67.

Authors

Gideon Rajan, he received the B.S degree in Information Technology from the Bharathidasan University, Trichy, India, in 2003 and the M.S degree from Madurai Kamaraj University, Madurai, India in 2005. Currently he is doing his Ph.D scholar in the Division of Electronics and Information Engineering at Chonbuk National University, Jeonju, S. Korea.

His current research interests include network architecture, network security, wireless sensor networks, routing protocols and key management.

Gihwan Cho, Prof. Cho received the B.S. degree from Chonnam University, Gwangju, Korea, in 1985, and the M.S. degree from Seoul National University, Seoul, Korea, in 1987, both in computer science and statistics. He received Ph.D. degree in computer science from University of Newcastle, Newcastle Upon Tyne, England, in 1996.

He worked for ETRI, Daejeon, Korea, as a Senior Member of Technical Staff from Sep. 1987 to Aug. 1997, for the Dept. of Computer Science at Mokpo National University, Mokpo, Korea, as a full time lecture from Sep. 1997 to Feb. 1999. From Mar. 1999, he joined to the Division of Computer Science and Engineering at Chonbuk National University, Jeonju, Korea. His current research interests include mobile computing, computer communication, security on wireless networks, wireless sensor networks. He is a member of IEEE, KIISE, KIPS, KMMS, KSII.