TWO-CHANNEL NON-INTERACTIVE MULTI-LEVEL KEY ESTABLISHMENT FOR BUNDLE SECURITY PROTOCOL OF DELAY/DISRUPTION TOLERANT NETWORKS (DTNS)

M. Srimathi[1] , M.Karthigha[2]

[1] PG scholar, [2]Assistant Professor, Department of CSE,
Sri Ramakrishna Engineering College, Coimbatore (India)

ABSTRACT

Protected, low-overhead key establishment is vital to maintain the high level of confidence and security that are necessary in several categories of Delay Tolerant Networks (DTNs). A small number of works presenting solutions to DTN key establishment have concentrated principally on targeted networking atmospheres. In this work, to deal with the key establishment concern for Bundle Protocol (BP), a time-evolving topology model and two-channel cryptography is formulated to design well-organized and non-interactive multilevel key exchange protocol. A time-evolving model is employed to properly model the periodic and fixed behaviour patterns of space DTNs, and consequently, a node can plan when and to whom it should transmit its public key. In the meantime, the application of two-channel cryptography allows DTN nodes to exchange their public keys or revocation position information, with authentication assurance and in a non-interactive approach. This approach facilitates to set up a secure context to maintain BSP, tolerating huge delays, and unanticipated loss of connectivity of space DTNs. The experimental investigation reveals the security and provides enhancement in peculiarities, problems and opportunities a DTN network maintenance.

***Keywords*: Bundle Authentication, Cryptographic Controls, Key Establishment, Space-Based Delay Tolerant Networks**

I. INTRODUCTION

Delay – Disruption Tolerant Architecture, DTN is meant to provide connectivity in Heterogeneous networks which lack incessant connectivity due to disruptions or considerable delays like that of networks operating in mobile or extreme terrestrial environments or planned network in space. The DTN effectively improves network communications where the network connectivity is Periodic/Intermittent and or Prone to disruptions [1]. The Store and Forward technique via the Bundle Protocol (BP) of the Delay Tolerant Network facilitates the flow of data/information across any complex or intermittent network traffic. Initially developed for Deep Space Communication (Inter Planetary Internet), the Delay-Disruption Tolerant Network communication model can also be used in Wireless (Terrestrial) environments, both in Military and Civilian Applications. The design of DTN and the protocol did not evolve without consideration for security which led to the development of relevant security documentations [2] [3] to address DTN-related security issues. The security documentations highlight security requirements, define design considerations, identify possible threats as well as open issues.

From the DTN security documentations and the security analysis in [4,5], the identified threats this work is designed to address are masquerading, modification and replay.

The use of PKI is associated with constraints like authorization server unavailability and limited capabilities of certain nodes for cryptographic operations. The focus of this paper is to investigate how PKI concept can be used to provide an authentication solution that does not depend on server availability during post trust establishment network communication while taking the capabilities of the entities into consideration. The existing PKI based schemes in DTN are [5] and [6,7]. These schemes either use certificates and encourage large storage of security credentials or depend on server availability. Here utilized a time-evolving topology model and twochannel cryptography to design efficient and noninteractive key exchange protocol.

The contributions of this paper are summarized as follows: 1) Implementing traditional PKI to provide trust initiation/establishment; 2) introducing the proposed two-channel cryptography and out-of-band channels for PKI based certificate; 3) proposing a time-evolving model to formally model the periodic and predetermined links of space DTNs; and 4) evaluating the performance of the proposed and reference schemes through simulation.

II. TWO-CHANNEL CRYPTOGRAPHY AND OUT-OF-BAND CHANNELS

As above-mentioned, the BSP needs a way of distributing public keys to support for this specification. Generally, anon-interactive message authentication protocol uses two separate channels. One is a broadband insecure channel and the other is a narrow-band authenticated channel. Some practical narrow-band channels include Voice-over-Internet-Protocol (VoIP), data imprinting by a user, Near Field Communication (NFC), infrared, laser, or visible light between two devices [8]. The narrow-band channels are generally called as Out-Of-Band (OOB) channels [9]. What follows are the common assumptions on twochannel cryptography. A broadband channel is insecure and an adversary has full control over this channel. The adversary can eavesdrop any messages sent over the broadband channel, modify the messages sent via this channel, and insert a forged message into this channel at any time that it likes. On the other hand, an adversary has limited control over the narrow-band authenticated channel. In detail, the adversary cannot modify the information transmitted over the narrowband authenticated channel. Balfanz et al. introduced the idea of hashing the data to be authenticated and delivering the hash value over the narrow-band authenticated channel to the verifier [10].In Figure 1, a broadband insecure channel is denoted by a single arrow line and a narrow-band authenticated channel is denoted by a double arrow line. In practice, the narrow-band channels are generally derived from OOB channels, which can be used in space DTNs context for bootstrapping security contexts and exchanging public keys. There are several issues that need to be addressed, such as, the balance between usability and security, the adaptation to diverse scenarios and contexts. A laser channel is used for implementing an OOB channel in space DTNs. In addition, the major merits of OOB channels are message integrity and authentication, instead of confidentiality.

2.1 Design of Network Model and Adversary Model

In this section, the network model and the adversary model is described, followed by design goals.

2.1.1 Network Model

In this work, space DTNs which can bridge between heterogeneous subnetworks using the Bundle Protocol suits are considered. Such a space network is recognized as evolving over time, i.e., its topology changes when some nodes appear, disappear because of being sheltered by celestial bodies, or move around. For space DTNs, this time-evolving property is periodic and predetermined. Given the prior knowledge pertaining to the relevant movement of celestial bodies and the positions of ground-based network nodes, space DTNs can be modelled by utilizing the time-evolving topology model. At least, ground stations and relay satellites with predetermined orbits can offer a deterministic framework which serves as the backbone for space networks.

In case of scheduled and periodic contacts, the public key exchange, update and the issuing of revocation status can be implemented based on time evolving network models combined with two-channel message authentication mechanisms, since OOB channels are easy to be achieved owning to the periodic and predetermined security aware contacts. In a time-evolving network model [11], a sequence of static graphs is needed to model this type of networks. As shown in Fig.1, each static graph is a snapshot representing nodes and the contacts between them at a certain moment. In this diagram there is no end-to-end path between some node pairs at one time-step, and the network is not connected at some time-steps as well. Then, the dynamic network with a sequence of snapshots is able to describe the evolution of the topology and the node mobility over a period of time.

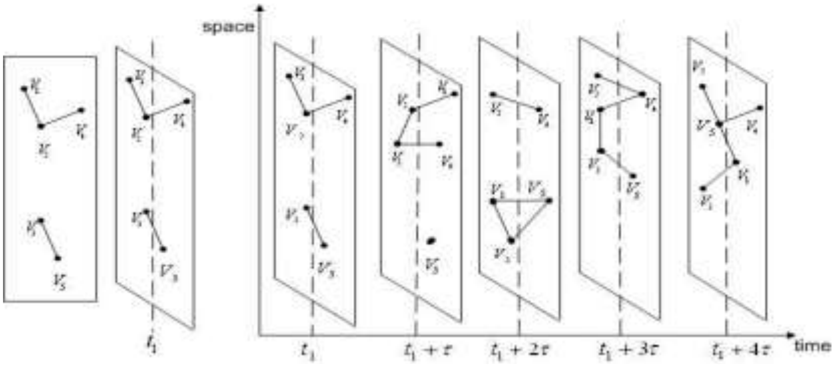


Fig.1. Time-Evolving Model of Dtns

2.1.2 Adversary Model

Consider that the adversary’s objective is to make the receiver (Bob) accept a public key PK along with the identity of the sender (Alice), when the public key PK was never sent by Alice to Bob. Two main types of attacks are considered: impersonation attacks and substitution attacks. An impersonation attacker attempts to convince the receiver (Bob) that a public key PK is sent from the sender (Alice), but Alice never sent PK and this session is factually initiated by the adversary. Here, note that, according to the model, the adversary cannot modify the data delivered over the narrowband authenticated channel, but he/she can replay this data.

2.1.3 Design Goals

Design goal is to address the key management issue of BSP for space DTNs, and to design a public key exchange protocol that will replace the application of any conventional online key distributing protocol or PKI. Specifically, aimed at making a public key generally-available, updating a public key, and repealing a public key, without resorting to the conventional mechanisms such as online key distributing, shared secrets, PKI, or trusted third parties. Here, a public key exchange protocol is a protocol that is used to exchange authentic copies of public keys between nodes.

2.2 The Proposed Scheme

The current BSP is built on the assumption that the DTN nodes already have access to authenticated copies of each other's public keys. That is, the DTN nodes know who they are supposed to be talking to. This assumption can be achieved by combining pre-authentication with periodic key exchange via OOB channels. In this section, proposed public key establishment scheme which will provide a fundamental key management support for BSP of space DTNs. The scheme consists of two stages: a bootstrap stage and an exchange stage.

2.1.2 Initiating and Bootstrapping Security Contexts

In this paper, pre-authentication mechanism is preferred to use to bootstrap the secure contexts for BSP secure communications. At bootstrapping stage, by exploiting two-channel cryptography techniques, the authentication information comes directly and demonstratively from their owners via authenticated OOB channels, and then the legality of this information can be confirmed easily. With respect to pre-authentication for space DTNs, an appropriate OOB channel is considered to be a manner with human attention. What this means is that the parties exchange key information via physical contacts (a type of authenticated OOB channels), such as injecting authenticated public keys by space mission authority, which is able to support demonstrative and authoritative identification. Another candidate OOB channel is audio band or vision band between two nodes. The demonstrative properties of such OOB channels with human attention enable a target device to be identified in communication. The key information that is established via such physical contacts during pre-authentication will then is used for subsequent secure communication using BSP.

2.3 Non-Interactive Multi-Level Key Establishment

NMKE is based on multi-variate symmetric polynomials, which was first proposed in [12] for group key agreement. In particular, at the initialization stage of NMKE, the root node of the hierarchy generates a ran- dom six-variate polynomial $\mathcal{F}(x_1; x_2; x_3; y_1; y_2; y_3)$ (referred to as the *master polynomial*) in the finite field $F_q, s.t., \mathcal{F}(, x_i, \ldots, y_i;) = \mathcal{F}(; y_i; ; ; x_i;), i = 1; 2; 3$. For each node *A* at the second level, the root node assigns a public identifier *IDA* to *A* and gives *A* a five-variate polynomial share $\mathcal{G}_A(x_2; x_3; y_1; y_2; y_3) = \mathcal{F}(ID_A; x_2; x_3; y_1; y_2; y_3)$. Then *A* further distributes four-variate polynomial shares to its chil- dren nodes (say *B*), $\mathcal{H}_B(x_3; y_1; y_2; y_3) = \mathcal{G}_A(IDB; x_3; y_1; y_2; y_3)$. Finally, a leaf node *C* that is a child of *B* obtains a three- variate polynomial share $U_C(y_1; y_2; y_3) = \mathcal{H}_B(ID_C; y_1; y_2; y_3)$.

In NMKE, each node has an unique identification vector (IV), which consists of three elements and is used for key establishment. The root node's IV is (null; null; null), where the value of null is equal to 1. The IV of a second-level node A is $(ID_A; null; null)$, and a third-level node B whose parent is A has the IV $(ID_A; ID_B; null)$. $(ID_A; ID_B; ID_C)$ is the IV of C, which is a child of B. To compute a secret key, each node evaluates its polynomial share by fixing all x's (if any) to be null and setting all y's as the elements of the other node's IV. For example, when C attempts to establish a shared key with a second-level node D, C computes$K_{C,D} = U_C(ID_D; null; null) = \mathcal{F}(ID_A; ID_B; ID_C; ID_D; null; null)$, while D computes$K_{D,C} = \mathcal{G}_D(null; null; ID_A; ID_B; ID_C) = \mathcal{F}(ID_D; null; null; ID_A; ID_B; ID_C)$.

Due to the symmetry property of $\mathcal{F}(x_1; x_2; x_3; y_1; y_2; y_3)$. $K_{C,D} = K_{D,C}$.

The above construction can only achieve partial resistance to collusion attacks at each level. To address this problem, Random Perturbation Polynomials (RPPs) is added to the polynomial shares that are distributed to third-level nodes and leaf nodes. The purpose of this is to prevent the attacker from getting the original polynomial shares, which are the essences of breaking the master polynomial. In particular, A generates (for its child B) a four- variate perturbed polynomial share

$\mathcal{H}'_B(x_3; y_1; y_2; y_3) = \mathcal{H}_B(x_3; y_1; y_2; y_3) + h_B(x_3; y_1; y_2; y_3)$ where $h_B(x_3; y_1; y_2; y_3)$is a RPP with r-bit outputs, $r < l = \lceil \log_2 q \rceil$ and $\mathcal{H}_B(x_3; y_1; y_2; y_3) = \mathcal{G}_A(ID_B; x_3; y_1; y_2; y_3)$. Similarly, C obtains $U'_C(y_1; y_2; y_3) = U_C(y_1; y_2; y_3) + u_C(y_1; y_2; y_3)$. Due to the existence of RPPs, the least significant r bits of the outputs of polynomial evaluations are perturbed. Hence, the most significant $l - r$ bits of the outputs are used as the key. If the $(l - r)$ bit key segment is not long enough to resist brute-force-based attacks, multiple master polynomials can be used simultaneously and concatenating these key segments can form a strong cryptographic key.

The design of RPPs is combining Lagrange interpolation and the construction algorithm for univariate perturbation polynomials. Let $I_1; I_2; I_3$ denote the domains of $x_1; x_2; x_3$ $(or\, y_1; y_2; y_3)$, respectively. In other words, I_i is the set of identifiers of the nodes at the $(i + 1)$-th level. Let JX denote the set of identifiers of X's children. In NMKE, the RPP for a four-variate polynomial share (of node B) is constructed as $h_B(x_3; y_1; y_2; y_3) = \sum_{i=1}^{\lambda} \alpha_B, i\,(x_3) \cdot \beta_B, i(y_1) \cdot \psi_i(y_2; y_3)$

where,

- $\alpha_{B,i}(x_3), i \in [1, \lambda]$ is a r_1 bit RPP constructed on the fly using Lagrange interpolation with randomly picked data points $\{(c_j, d_j): c_j \in \mathcal{J}_B, d_j \in_R [0, 2^{r_1} - 1]\}$
- $\beta_{B,i}(y_1), i \in [1, \lambda]$ is a r_2-bit RPP constructed on the fly using Lagrange interpolation with randomly picked data points$\{(e_j, f_j): e_j \in I_1, f_j \in_R [0, 2^{r_2} - 1]\}$
- $\psi_i(y_2; y_3), i \in [1, \lambda]$is a r3-bit RPP pre-computed using the algorithm

Note that the degrees of $\alpha_{B,i}(x_3)\ and\ \beta_{B,i}(y_1)$ are $|\mathcal{J}_B|$ and $|I_1|$, respectively, which are fairly small since there are limited number of nodes (resp. children) at the first level (resp. of B). Furthermore, the construction algorithm ensures that $\psi_i(y_2; y_3)$can have a small degree and scale to potentially large domains ($i.e., I_2 \times I_3$). The perturbation length of $h_B(x_3; y_1; y_2; y_3)\ is\ r = r_1 + r_2 + r_3$. Similarly, the construction of three-variate RPP for leaf node C is $u_C(y_1; y_2; y_3) = \sum_{i=1}^{\lambda} \beta_{C,i}(y_1) \cdot \psi_i(y_2; y_3)$

III. NON-INTERACTIVE MULTILEVEL PUBLIC KEY EXCHANGE FOR SPACE DTNS

In addition to initiating and bootstrapping as above described, the DTN nodes need to exchange and update their public keys periodically in the future life of the network. In the proposed scheme, the network nodes implement this process not blindly, but according to schedule. The schedule model is derived from space-time graph that illustrates security-aware contacts between space DTN nodes at certain time steps. When a period for exchanging or updating comes, each DTN node sends its public key and the authentication information for this key to the security-aware neighbors, according to a predetermined space-time graph. In the following subsections, first presented the non-interactive *multilevel*public key exchange protocol using two-channel cryptographic technologies, and then introduce the space-time graph for space DTNs. Thereafter, the public key exchange mechanism based on space-time graphs is given.

3.1 Public Key Exchange Protocol

Due to high delays and unexpected loss of connectivity, an interactive protocol does not work well in space DTNs. This motivates a design of non-interactive *multilevel*key exchange protocols in an authenticated manner. As discussed above, two-channel cryptography and OOB channels have advantages on designing a non-interactive *multilevel*message authentication protocol, which utilized to enable two DTN nodes to securely exchange their public keys (or revocation status information). The main idea is to exchange a public key, that may be long term or ephemeral, on the normal channel, and independently calculate a cryptographic hash value from this public key. This hash value is then transmitted from one device to the other over the OOB channel, in order to verify that the public key exchanged on the normal channel has not been altered. Because of only processing at security-aware nodes, i.e., a "single hop" from a security-aware forwarder to the next security-aware intermediate receiver [13], an authenticated OOB is easily achieved. Accordingly, by utilizing two-channel cryptography, public keys can be authenticated between a forwarder and the next intermediate receiver, if it is needed. Here considered a space node V_i that possesses the public key PK_i and performs the following protocol. This protocol enables V_i to securely send its public key PK_i to another node V_j which is reachable in one hop for V_i. In more detail, the protocol is performed as follows:

1) The sender, V_i, appends its identity ID_i as well as the current time t to its public key PK_i, and thereafter sends the result $PK_i \| ID_i \| t$ to the receiver V_j over a broadband insecure channel (a traditional channel);

2) The sender, V_i, computes $h = H(PK_i \| ID_i \| t)$

3) The sender, V_i, sends the authentication information for its public key, i.e., h, to the receiver V_j over the narrowband authenticated channel (often OOB channels);

4) When receiving the public key $PK_i{}' \| ID_i{}' \| t'$ and the authentication information h' for this public key from V_i over the traditional channel and the OOB channel respectively, the receiver V_j accepts PK_i as the public key of V_i if t' is the correct timestamp and $h' = H(PK_i{}' \| ID_i{}' \| t')$; otherwise, reject it.

Further illustrated this process in the following Fig.2. Here, *H* is a collision resistant hash function. In order to resist birthday attacks, the size of *h* needs at least 160 bits. Mashatan and Stinson gave a formal security proof for the non-interactive *multilevel*message authentication protocol on which the above key exchange protocol is built [14].In addition, in this protocol introduced timestamps to protect it from replay attacks since it is a one-pass protocol and inherently open to replay attacks. This means that nodes would need to have a common notion of time, just as precisely determining windows of communication opportunities and correct antenna-pointing, for example. The time synchronization issue is one of the current areas of space DTN research. Most works aim at using suitable modifications to the Network Time Protocol (NTP) and the CCSDS Proximity-1 Space Link Protocol. NTP is widely used to synchronize computers in the Earth Internet and has been deployed in low-orbit Earth orbiters. In this paper, assumed that space DTNs have time synchronization.

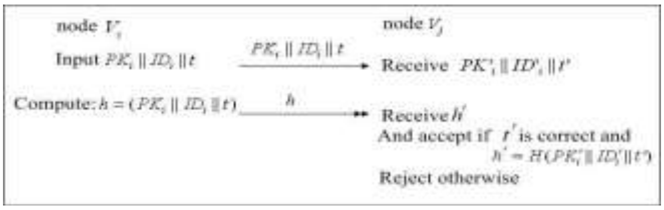

node V_i
node V_j
Input $PK_i \| ID_i \| t$
$PK_i \| ID_i \| t$
Receive $PK'_i \| ID'_i \| t'$
Compute: $h = (PK_i \| ID_i \| t)$
h
Receive h'
And accept if t' is correct and
$h' = H(PK'_i \| ID'_i \| t')$
Reject otherwise

Fig.2. Non-interactive multilevel public key exchange protocol

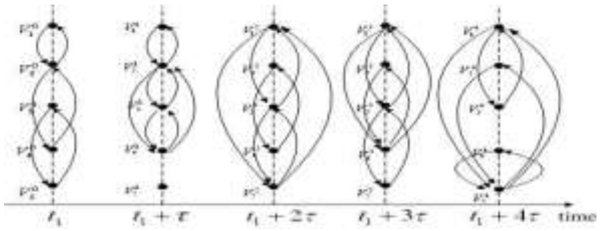


Fig.3. Space-time graphs for space DTNs

IV. SPACE-TIME GRAPHS BASED PUBLIC KEY EXCHANGE FOR SPACE DTN

Now the public key exchange protocol is described based on the above-generated space-time graph specifying when and to whom a node should send its public key. When a period comes, say t_1, the process for public key exchange is started. According to the space-time graph, each node sends its public key to all the predictable nodes reachable in one hop, via the non-interactive protocol given by Fig.2. Each node V_i, i = 1,..., n performs as follows (used "→" to denote the protocol given in Figure 3):

1) At time t_1, $V_i \rightarrow V_{j1}$, when the node V_{j1} is one-hop reachable for $V_i$at this moment;

2) At time $t_1 + \tau$, $V_i \rightarrow V_{j2}$, when the node V_{j2} is onehop reachable at this moment and not one-hop reachable at the preceding moment t_1;

3) At time $t_1 + 2\tau$, $V_i \rightarrow V_{j3}$, when the node V_{j3} is onehop reachable at this moment and not one-hop reachable at the preceding moments t_1 as well as $t_1 + \tau$ (i.e., not one-hop reachable at all the preceding time points in the time dimension of the space-time graph); and so on.

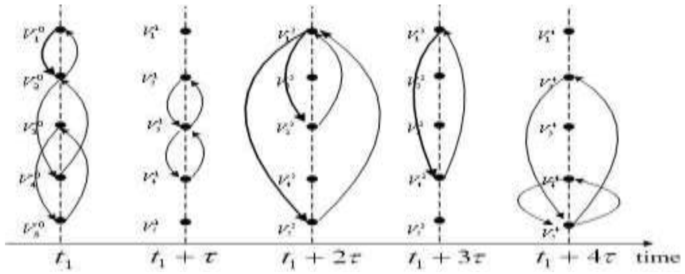


Fig.4. Public key exchange based on space-time graph

As shown in Fig.4, a directed arc line $v_{i,j}^t$ denotes that node $V_i$sends its public key and the corresponding authentication information to one of its one-hop reachable nodes $V_j$at time t, by utilizing a two-channel cryptography technologies. For node V_1, at time t_1, it sends its public key to node V_2 in a non-interactive and authenticated manner, since V_2 is its one-hop reachable node at that moment. At time $t_1 + 2\tau$, V_1 sends its public key to V_3 and V_5 respectively.

Then, at time $t_1 + 3\tau$, V_1 sends its public key to V_4. Thus, all the other nodes in this network have gotten the public key of node V_1. Illustrated this process with bold arc lines.

From another perspective, at time t_1, key exchange takes place between three pairs (V_1, V_2), (V_2, V_4) and (V_3, V_5). At time $t_1 + \tau$, key exchange takes place between $V_2$and V_3, as well as V_3 and V4. Then, at time $t_1 + 2\tau$, two pairs, (V_1, V_3) and (V_1, V_5), perform this key exchange protocol. Only one pair (V_1, V_3) exchanges keys at time $t_1 + 3\tau$. At time $t_1 + 4\tau$, there are two pairs, (V_2, V_5) and (V_4, V_5), performing public key exchange process. Finally, it is seen that all nodes in the network given in Fig.1 complete public key exchange in four slots from

t_1.It is important to note that the similar method can also be applied to exchange public key revocation messages between space DTN nodes. In this way, the authentication and integrity of public key revocation message can also be guaranteed. This is another essential issue of secure space DTNs [15].

With the scheduled and periodic contacts, the public key exchange, public key update and the revocation status issuing can be implemented based on time-evolving network models combined with two-channel message authentication mechanisms. Unlike the traditional PKI, here it does not need a Certification Authority (CA) and no certificate is involved. Via the above mechanism, the backbone network, including DTN gateways that connect various DTN domains, achieves the support of generally-available public keys. Nevertheless, there are still some nodes that might never be in contact with some others. Considering this case, let the DTN security gateways to bridge between the nodes in the backbone network and the nodes in the sub-networks. This means a hierarchical strategy. Specifically, the backbone network and the access sub-network respectively run the above protocol interiorly. A DTN security gateway forwards the public keys from the nodes in the domain or sub-network that the gateway controls to the nodes in the backbone network, along with its own public key. Meanwhile, the gateway also forwards the public keys of the nodes outside of the sub-network to the nodes in the sub-network that it controls.

4.1 Security Consideration

In the public key exchange protocol (Figure 3) based on two-channel cryptography, $PK_i \| ID_i \| t$ and its corresponding hash value$h = H(PK_i \| ID_i \| t)$ respectively correspond to the message M and its hash value in the protocol given in Figure 1. A formalssecurity proof for this protocol, on which the key exchange protocol is built, is given by Mashatan and Stinson [10]. Here just briefly sketched the key points specifying the security of the scheme. Two types of attackers are defined as follows: substitution attackers and impersonation attackers, in order to show that the receiver can assure the owner of the public key, and its authenticity as well as freshness.For a substitution adversary, it is computationally infeasible to find a substitution $PK_i' \| ID_i \| t$ such that$H(PK_i' \| ID_i \| t) = h$.Here, $PK_i'$is a false public key. This is implied from the assumption that the adversary cannot modify the information (i.e., h) transmitted over the narrow-band authenticated channel.

What is more, H is a collision resistant hash function. In order to resist birthday attack, the size of the authenticated information h is greater than 160 bits.According to the two-channel cryptography, an adversary cannot forget the authentication information sent over the narrow-band authenticated channel. Then, for an impersonation adversary, in order to convince the receiver that a public key $PK_i' \| ID_i' \| t$ is sent from a target sender, it has to replay the authentication information previously sent by the target sender, such as$h' = H(PK_i' \| ID_i' \| t')$. Here note that t is the current time and t'represents the preceding time. Factually, this type of attacks are successful with negligible probability, because it is computationally infeasible to find a forged $PK_i' \| ID_i' \| t$ such that $H(PK_i' \| ID_i' \| t) = h'$, even if $PK_i' \| ID_i' = PK_i \| ID_i$. This is derived from the assumption that H is a collision resistant hash function and the size of the hash value is greater than 160 bits.

V. EXPERIMENTAL RESULTS AND DISCUSSION

To examine the performance of the proposed scheme, simulations have been conducted to evaluate the convergence speed. In this simulation, convergence speed is considered as a metric for the performance measurement. The convergence means that every node achieves the public keys of all the other nodes during a key exchange period. The convergence speed is measured by the minimum number of slots during which all nodes in the network complete public key exchange. In this simulation, the experiment is repeated for multiple times and obtained the average values of this metric. Randomly a time-evolving network is generated via random graph model.

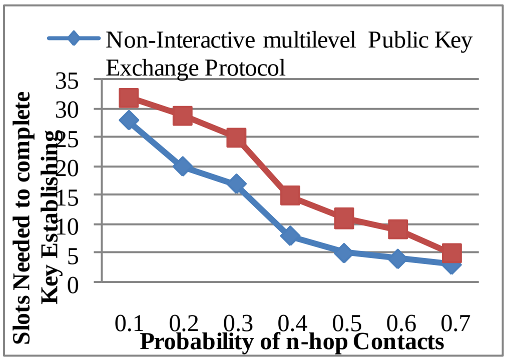


Fig.5. Convergence Speed Comparison

First a sequence of static random graphs is gnerated in order to represent the time-evolving DTN with 100 nodes. Then, the space-time graph corresponding to this time-evolving network is generated, and thereafter the public key exchange process is performed on this spacetime graph. In this experiment, probability *p*increasedfrom 0.1 to 0.99 which significantly increses network density. For each probability, 100 random networks and get an average value is generated, which is presented in Fig.5.

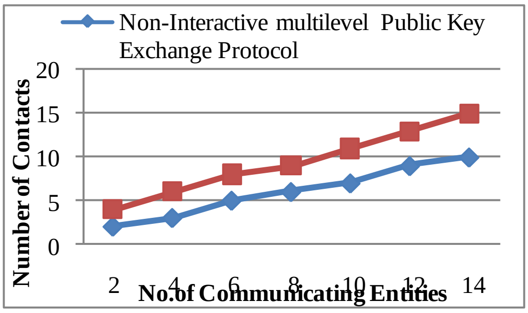
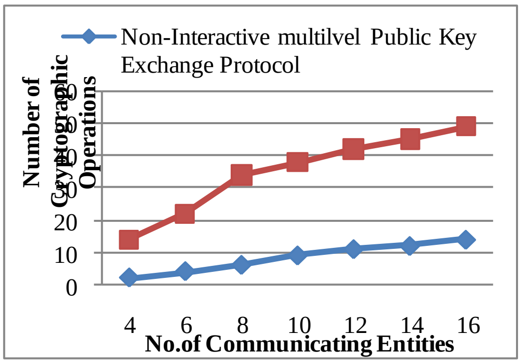


Fig.6.Simulation result for Number of Contacts

Fig. 6 shows the simulation result for the number of contact of the communicating entities with proposed system. From the figure when the number of communicating entities increases the number of contacts also increases. The proposed system hasfewer contacts when compared to the existing one. The reason is that the convergence speed of theproposed system is high



.

Fig.7.Simulation result for Number of Cryptographic Operations

Fig.7 shows the number of cryptographic operations carried out by proposed system during bundle transmission. The number of communicating entities include one sender, one destination and as many intermediate nodes (DM) as possible. While the proposed scheme has zero contact and zero cryptographic operations by the proposed system, the number of contacts and cryptographic operations by proposed system reduces with increase in the number of communicating entities.For every contact establish proposed work carries out three cryptographic operations of public key decryption, signature verification and symmetric key encryption.

VI. CONCLUSION

In this paper, a novel approach non interactive public key exchange protocol is proposed along with some directions for addressing the challenging problem of Non-Interactive multilevel Key establishment in space DTN environments and establishing secure context to support for BSP of space DTNs. As the DTN is relatively new, the current state of the art is mainly limited to the “language” the security nodes should speak upon which the security services would be built. Limited work has been done in the area of key management and more specifically in key exchange. In the proposed protocol, the space-time graph is utilized to model the predictable property of space networks. This makes the key establishment process scheduled and not opportunistic. The performance of the proposed protocol is measured by means of convergence speed, cryptographic operations and number of context. The experimental results shows that the proposed protocol is better than the existing public key exchange protocols in delay tolerant networks

REFERENCES

[1] Artemios G. Voyiatzis, “A survey of delay – disruption tolerant networking applications”, Journal of Internet engineering, Vol 5 no 1, pp: 331-343, June 2012.

[2] Farrell, S., Symington, S., Weiss, H., Lovell, P.: Delay-Tolerant Networking Security Overview. IETF Internet Draft, draft-irtf-dtnrg-sec-overview-06 (2009)

[3] Symington, S., Farrell, S., Weiss, H., Lovell, P.: Bundle Security Protocol Specification. IETF Internet Draft, draft-irtf-dtnrg-bundle-security-15 (2010)

[4] Farrell, S., Cahill, V.: Security Considerations in Space and Delay Tolerant Networks. In: Second IEEE International Conference on Space Mission Challenges for Information Technology (2006)

[5] Jia, Z., Lin, X., Tan, S. H., Li, L., & Yang, Y. (2012). Public key distribution scheme for delay tolerant networks based on two-channel cryptography. Journal of Network and Computer Applications, 35(3), 905-913.

[6] Basha, J. A., & Mozhi, D. A. (2014). Detection of Misbehaviour Activities in Delay Tolerant Network Using Trust Authority, Volume 2, Issue 2, pp.1864-1868.

[7] Johari, R., & Gupta, N. (2011, October). Secure query processing in delay tolerant network using java cryptography architecture. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on (pp. 653-657). IEEE.

[8]Fall, K..: A Delay-Tolerant Network Architecture for Challenged Internets. In: SIGCOMM’ 03, August 25-29, 2003, Karlsruhe, Germany

[9] Asokan, N., Kostiainen, K., Ginzboorg, J. Ott and C. Luo.: Towards Securing DisruptionTolerant Networking. Nokia Research Centre, NRC-TR-2007-007 (2007)

[10] Mashatan and D. Stinson, “Practical unconditionally secure twochannel message authentication,” Designs, Codes Cryptogr., vol. 55, no. 2, pp. 169–188, 2010.

[11] R. Kainda, I. Flechais, and A. Roscoe, “Usability and security of outof-band channels in secure device pairing protocols,” in Proc. 5th Symp.Usable Privacy Sec., 2009, pp. 1–12.

[12] Balfanz, D. Smetters, P. Stewart, and H. Wong, “Talking to strangers: Authentication in ad-hoc wireless networks,” in Proc. 9th Annu. NDSS, 2002, pp. 7–19.

[13] M. Huang, S. Chen, Y. Zhu, and Y. Wang, “Cost-efficient topology design problem in time-evolving delay-tolerant networks,” in Proc. IEEE Global Telecommun. Conf., Dec. 2010, pp. 1–5.