Literature Review on Security Aspects of Delay Tolerant Networks

Ankita Nayal
M.Tech Scholar
Computer Science Department
Maulana Azad National Institute of Technology, India

Sweta Jain
Assistant Professor
Computer Science Department
Maulana Azad National Institute of Technology, India

ABSTRACT
In the past few decades, Delay Tolerant Networks (DTNs) have emerged as one of the hot topics for research. It is a network, used in environments where end to end connectivity is unavailable. It has no fixed infrastructure and has scarce resources. DTNs use store and forward technique which is called opportunistic data forwarding. One of the most important aspects of DTNs is security, because they are a new network paradigm and should be acceptable by all. This paper discusses the works related to DTN security, their analysis, drawbacks, comparisons, advantages and other factors.

Keywords
Security, Delay Tolerant Networks (DTNs), disconnected environments.

1. INTRODUCTION
DTN was introduced mainly for interplanetary communication to deal with issues like delays and packet corruption, but now it has a wide range of applications.

In DTNs messages are broken into bundles. This network has three main components:

1. **Host**: sends or receives bundles.
2. **Router**: forwards bundles to same region
3. **Gateway**: forwards bundles to other regions.

The Bundle layer uses Bundle Protocol **[1]** which deals with problems of acknowledgements due to disconnected environments, the Bundle layer **[2]** acts as bridge between application and transport layer **(see Figure 1).** This paper discusses the security related issues, and related work in the field of DTN security.

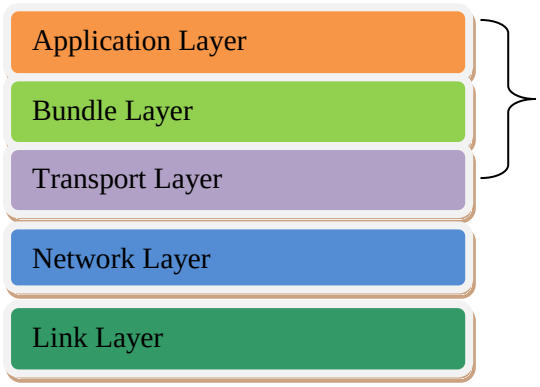

Figure 1: Bundle layer between application and transport layer

2. DTN SECURITY
The security for DTNs has to be very strong because the forwarding nodes in between can be compromised very easily. For security in DTN, the bundle has three security headers or blocks **[3].** The three security headers are as follows:

1. Bundle Authentication Header: This block or header checks the bundle is authenticate or not, this authentication takes place for every hop.

2. Payload security header or Payload integrity block: Checks integrity of payload of bundle, in other words checks whether the message has been modified or is the original one.

3. Confidentiality block for payload: This is to keep the payload secret or confidential, for this the payload is first encrypted and then encapsulated

3. AUTHENTICATION, INTEGRITY AND CONFIDENTIALITY
According to Ashokan et al. **[4]** In DTNs environment, authentication, integrity and confidentiality are very important factors because sender has to authenticate and decide whether it has to forward the message or not, it forwards the message from certain chosen senders only, and receiver has to authenticate sender in order to interpret the message accordingly.

Confidentiality in DTNs requires key management. Conventional methods like Public Key Infrastructure (PKI) do not work well in DTNs because data is encrypted through session key, and then session key is in turn encrypted with the receiver's public key, which cannot be obtained because of disconnected environments; ultimately the communication cannot take place.

DTNs are vulnerable to various different kinds of attacks; the following table **(see Table 1)** enlists the attacks and their working.

Table 1: Attacks and their working

Attacks	How it works
Blackhole attack	A node advertises itself as a valid node by creating forged bundles and then drops them; it advertises having the shortest path to the destination. It is also known as packet dropping attack.
Wormhole attack	A node forwards bundles through a high quality out-of-band path and replays them to another node at another location in the network.

Grayhole attack	A correct node changes its behavior to a blackhole node.
Replay attack	Launch replays to consume the resources
Identity Theft attack	The third party pretends as receiver and receives the message meant for the receiver
Sybil attack	It ruins the reputation by making fraudulent identities or imitating identities.
Whitewashing attack	A node with bad reputation makes a re- entry in the network with a fresh identity
Cooperative attack	Cooperative attack is done by nodes that involve other nodes to launch attacks

4. RELATED OPEN ISSUES

1. Key management: As we have already discussed, PKI is highly impractical in DTN, because it requires key distribution through online servers or an online service which is quiet impossible in DTNs because of the disruption.

2. Analysing the traffic: The extent up to which analysis has to be done and how to make it less resource exhaustive remains an open issue.

3. Multicast security and handling replays: DTN allows unlimited number of registrations in an endpoint, even if that node is singleton, more than one node can come and register and receive the messages meant for that node. Handling replays remain an open issue because of delays in DTNs. **[5]**

4. Flexibility: Flexibility remains an open issue. The bundle in bundle encapsulation mechanism for confidentiality has high complexity and requires high cost. [**6]**

5. DTN SECURITY RELATED WORKS

Several significant works have been done related to security in DTNs. Some of the related works are discussed here:

PKI **(see Figure 2)** cannot be implemented in DTNs; because of disconnectivity that is why a new cryptographic method called Identity based cryptography (IBC) came into existence which was first given by Boneh and Franklin **[7].** Ashokan et al compared the conventional public key cryptography with IBC and gave the results as in **Table 2**

Table 2: Comparative analysis IBC and PKI

S.No	CCM	IBC
1	There is a requirement of availability of online servers for key at the time of reception.	There is no requirement of availability of online servers for key at the time of receiving. IBC key can be obtained earlier.
2	Only one public key is required to encrypt for every receiver.	Separate encapsulations of public key are required for different receivers.

Ashokan et al. also did the comparison between the conventional cryptography methods CCM (Conventional cryptography methods) and IBC (Identity Based Cryptography). The summary of the comparison is presented in **Table 3.**

Table 3: Comparative analysis of CCM and IBC

Property	IBC	PKI
Authentication	Effectiveness same as PKI	Effectiveness same as IBC
Confidentiality	Better than PKI	PKI has a lower hand as compared to IBC

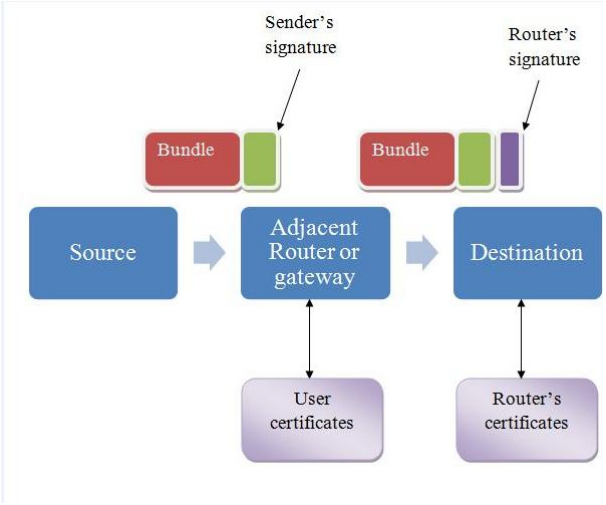

Figure 2: Public Key Infrastructure

Thus, it was concluded that IBC has no big or important advantage over conventional or traditional cryptographic methods. IBC proves to be useful or has an upper hand over the traditional methods only in case of confidentiality.

One more significant work in the field of IBC is done by Seth et al **[8].** It includes a security design on the basis of HIBC (Hierarchical IBC). In HIBC, public key can be the public ID like email address or username concatenated with the region to which the user belongs which depends on the hierarchy of regions.

Private Key is obtained through Private Key generator (PKG). Each region has a PKG. They introduced a novel method of generating time based keys for their usage in case of identity theft, when any mobile device is lost. They introduced the concept of "USB keys" which assists PKG to distribute the keys to any user which cannot access online service or is disconnected and is not able to access the keys, but they do not discuss the methodology of how they will authenticate the genuine users before distributing the keys, they only assumed that the verification of user's email ID will be done for authentication.

As can be seen through **Table 1** DTNs suffer from various kinds of attacks, many research papers have been published to thwart these attacks and to find the solutions for them. Some of them are discussed here.

Godwin Ansa et al. **[9]** proposed a DTN cookie mechanism to identify and filter out illegal traffic. Three variants of DTNs cookie for Intra Regional Denial of service (DOS) alleviation are proposed where it is assumed that the sensor network are divided into domains, a group head node and a security aware node. NTL (network threat level) is mapped with the related DTN cookie variants. Based on the NTL; the Bundle Protocol Agent decides which cipher has to be chosen to check the DTN cookie. The security aware node maintains a list of malicious nodes. If the authentication process is failed thrice, an alert is sent to the group head node which contains the cookie matching with the NTL. Egress filtering is then applied at security gateways. Similarly, this technique is used for Inter Regional DOS with slight variation in DTN cookies where instead of egress, ingress filtering was used. Basic drawback of this approach includes using of HMAC for one of the cookie variants, which is too much complex and costlier than other hash functions. Also it is assumed that the security gateways have large space which is not practical in DTNs because of resource constraints.

The nodes in DTNs follow cyclic patterns. These cyclic patterns can make up the contact history of the node, this history can be used to know the number of contacts made with a particular forwarding node to know its suitability to forward the bundles, but this can be exploited by the malicious attackers to take undue advantage. So, there is always a need of a strong mechanism required for predicting the contacts. But, Blackhole attack poses problems for it. Therefore, Feng Li et al **[10]** proposed Encounter Tickets and Encounter Prediction to mitigate Black hole attack. A definition of Encounter Tickets was given as an entity that proves that two nodes encountered at time T. Simulation studies were conducted to evaluate the effectiveness of Encounter tickets, in preventing Blackhole attacks. The results of the paper are summarised as follows **(see Table 4)**

Table 4: Comparative analysis between Encounter Prediction, MaxProp and Random in terms of Delivery rate

Protocol	Delivery rate without tickets	Delivery rate with Tickets
Encounter Prediction	Same as Random	Almost same as MaxProp and more than delivery rate without tickets
MaxProp	Lowest than the other two	Highest than the other two
Random	Same as Encounter Prediction	Lowest than the other two but almost same as delivery rate without tickets

Through the above results, it can be concluded that Encounter Prediction performs well as compared to the other two mentioned in both cases of with tickets or without tickets. The drawback of this paper is that this scheme cannot prevent dropping of packets and only prevents the attackers to prove false encounters, which is insufficient to mitigate Blackhole attacks.

Another problem that always shows up in DTNs is the "selfishness" problem. It is usually assumed in several studies and research works that the nodes in between the source and destination are always ready to forward the bundles, but unluckily in reality there may exist some selfish nodes which are uncooperative and do not help in forwarding the bundles. The reason behind this behaviour is DTNs resource scarcity, every node wants to save its resources (say for example: battery) and that's why they act selfishly.

To understand the solution of the selfish node problem, we take an example of real life, suppose there is a small boy, who is kind of stubborn and bad, to encourage him to grow up to be a good person, we reward him for his good deeds. Similarly when a selfish node will be forwarding the bundle, it's given a reward, or motivation called Incentives in DTNs.

There are basically three Incentive schemes in DTNs:

1. Reputation based -Generally, in reputation based scheme, the nodes which are cooperative attain good reputation from other nodes.
2. Credit based **[11]**-The selfish nodes are aroused to forward the bundles, they are encouraged by credits from the source node, if the bundle reaches successfully to the destination. The credits are generally virtual currency.
3. Tit for Tat based – In, tit for tat based scheme, the nodes will help only those nod**es** which help them and want much more services from others as compared to services which they provide to the others nodes, that is why they are unsuitable for DTNs

These incentive schemes suffer through various attacks, the summary is given in tabular form in **Table 5**:

Table 5: Incentive schemes and related attacks

Scheme	Attacks/Threats
Reputation based	1. **Sybil attack:** It ruins the reputation by making fraudulent identities or imitating identities. 2.**Whitewashing attack**: A node with bad reputation makes a re- entry in the network with a fresh identity
Credit based	The major threat here is dishonesty of the nodes.

Due to the nature of DTNs like opportunistic links, very few node contacts etc. It is quiet difficult to detect the selfish nodes. Therefore this area is open for research and many research papers have been published in this area. Rongxing Lu et al**. [12]** proposed a practical incentive for DTNs. It combines both Reputation and Credit based incentive schemes, it is proposed that if a bundle successfully reaches the receiver, then the adjacent neighbour node will get a credit from the source, and if the bundle is not delivered due to some failure, then also the node will get reputation from the trusted authority. Simulation results were given to show that the protocol works better in terms of delivery ratio and causes less delay when high incentive is given.

Lifei Wei et al. **[13]** proposed MobiID a different incentive scheme which is based on reputation based incentive scheme, except for the fact that it is focussed on the users and is socially aware because it notes down each and every data forwarding. MobiID allows the nodes to maintain their reputation proof and show whenever required. It introduced the concept of:

1. Self check: The reputation proof is kept by the node itself for future.
2. Community check: The reputation proof is kept by the network for future.

It defines a social parameter which considers the nodes which are ready to forward from the history of forwarding. It uses this property for the fast establishment of reputation.

6. CONCLUSION

This paper reviewed different aspects of DTNs and related works, with the hope that it will provide the readers especially the beginners an insight into the security related works being done in the field of DTNs. Topics like authentication, integrity, confidentiality, attacks related to prediction of contacts, denial of service mitigation, attacks related to incentive schemes were discussed, covering almost every point related to security .It will help the readers to know the related open issues and guide them to start their work, and contribute something to the field of DTNs.

Future work can be carried on with the open issues mentioned. Existing protocols have to be improved further for better security. Continuous and secure storage are also needed.

7. ACKNOWLEDGMENTS

I would like to express my immense gratitude to Ms. Sweta Jain for her support and guidance.

8. REFERENCES

[1] K. Fall, "*A Delay-Tolerant Network Architecture for Challenged Internets*," Proc. ACM Special Interest Group Data Comm. Workshop (SIGCOMM '03), 2003.

[2] V. Cerf, A. Hooke, L. Torgerson, R. Durst, K. Scott, K.Fall , H. Weiss "*Delay-Tolerant Networking Architecture*", IETF RFC 4838, Apr. 2007.

[3] S. Symington, S. Farrell, and H. Weiss, *Bundle Security Protocol Specification.* IRTF, DTN research group , October 2006. Draft version -02; expires in April 2007.

[4] N. Asokan, Kari Kostiainen, Philip Ginzboorg, Jorg Ott, Cheng Luo "*Applicability of Identity-Based Cryptography for Disruption-Tolerant Networking*" In MobiOpp '07: Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking, pages 52–56, New York, NY, USA, 2007. ACM.

[5] Bindra H., Sangal A "*Considerations and Open Issues in Delay Tolerant Network's (DTNs) Security*". Wireless Sensor Network Scientific Research Journal, pp. 635--648 (2010)

[6] Stephen Farrell, Vinny Cahill "*Security Considerations in Space and Delay Tolerant Networks"* In SMC-IT '06: Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology, pages 29–38, Washington, DC, USA, 2006. IEEE Computer Society.

[7] D. Boneh and M. Franklin, "*Identity-based encryption from the Weil pairing*," in CRYPTO 2001, Advances in Cryptology, no. 2139 in Lecture Notes in Computer Science, pp. 213–229, Springer-Verlag, August 2001

[8] A. Seth, U. Hengartner, and S. Keshav, "*Practical security for disconnected nodes*," in First Workshop on Secure Network Protocols (NPSec), November 2005. Revised 2006 version of the NPSec paper http://www.cs.uwaterloo.ca/_a3seth/

[9] Godwin Ansa, Haitham Cruickshank and Zhili Sun "*A Proactive DOS Filter Mechanism for Delay Tolerant Networks"2nd ICST PSATS, Conference*, Malaga Spain, February 2011

[10] Feng Li, Jie Wu, Avinash Srinivasan, "*Thwarting Blackhole Attacks in Distruption- Tolerant Networks using Encounter Tickets*" INFOCOM 2009, IEEE. IEEE 2009

[11] Bin Bin Chen, Mun Choon Chan "*MobiCent: A Credit-Based Incentive System for Disruption Tolerant Network*" In *INFOCOM, 2010 Proceedings IEEE,* pages 1–9. IEEE, 2010

[12] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xuemin (Sherman) Shen, Bruno Preiss "*Pi: A Practical Incentive Protocol for Delay Tolerant Networks"*IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 4, APRIL 2010

[13] Lifei Wei, Haojin Zhu, Zhenfu Cao, and Xuemin (Sherman) Shen "*MobiID: A User-Centric and Social-Aware Reputation Based Incentive Scheme for Delay/Disruption Tolerant Networks"* H. Frey, X. Li, and S. Ruehrup (Eds.): ADHOC-NOW 2011, LNCS 6811, pp. 177–190, 2011._c Springer-Verlag Berlin Heidelberg 2011