IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Security Trends in Delay Tolerant Networks

Audumbar T. Mohite[1], S.P. Sonavane[2]

Walchand College of Engineering, Sangli, MH, India[1, 2]

Abstract: Delay Tolerant Network (DTN) is a class of network which has high end to end latency, opportunistic communication and infrastructure less network. The selfish or malicious node may drops the received packet, due to such type of misbehavior the performance of network decreases. In this paper, the survey of security trends in Delay Tolerant Networks is reviewed. The various ways for dropped packet detection and routing misbehavior detection with an appropriate method are presented. It also focuses method for defending against flood attacks in DTNs, secure data retrieval scheme, design and validation of dynamic trust management protocol. The remark is also made with the overall analysis.

Index Terms: DTN, Security, Trusted Authority, Misbehavior Detection, Trusted Authority.

I. INTRODUCTION

The Delay Tolerant Network (DTN) is a type of network in which communication takes place without network infrastructure. In DTNs, the messages can be sent over an existing link and buffered at next hop. Whenever, the next hop comes in range, the message is transferred to that node. This message propagation is called as "store-carry-forward" i.e. when a node receives some packets and it stores these packets into its buffer, carries them around it until it contacts another node and then forwards the packets. In DTN, the routing is decided in an opportunistic way [1].

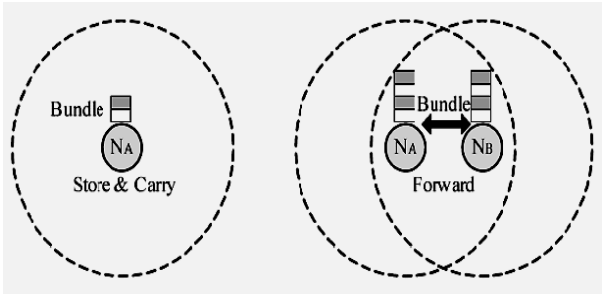

Figure 1: Bundle store-carry- forward in DTN [2]

As shown in figure 1, the bundles could only be forwarded when two DTN nodes (N_A ,N_B) move within each other's range and contact with each other during a period of time. If any other DTN node is not within the transmission range of DTN node N_A , then N_A will buffer the current bundles and carry them until other DTN node appears within its transmission range [2].

Due to the unique features of the DTN, such as lack of existing path and variation in network conditions, it is hard to detect node's selfish behavior [2].

In DTN, some of the nodes are selfish nodes that try to maximize their own benefits and refuse to forward the message to others. The another type of nodes as malicious nodes which drop or modify messages. Due to these the packet delivery ratio and performance of the DTN reduces considerably [1]. Hence, in DTN, misbehavior detection is important to assure the secure routing.

II. LITERATURE SURVEY

Zhu, Du [1] proposed a general DTN which is formed by a set of mobile devices owned by individual users. Each node i is assumed to have a unique nonzero identifier N_i, which is bound to a specific public key certificate.
The basic iTrust i.e. probabilistic misbehavior detection scheme has two phases, including Routing Evidence Generation phase and Routing Evidence Auditing phase. In the Evidence Generation phase, the nodes will generate contact evidence and data forwarding evidence for each contact or data forwarding by nodes. In the auditing phase, Trusted Authority (TA) will distinguish the normal nodes from the misbehaving nodes [1].

In the routing evidence generation phase, node A in figure 2 forwards packets to node B, then gets the delegation history back. Node B holds the packet and then encounters node C. Node C gets the contact history about node B. In the auditing phase, when TA decides to check node B, TA will broadcast a message to ask other nodes to submit all the evidences about node B, then node A submits the delegation history from node B, node B submits the forwarding history (delegation history from node C), node C submits the contact history about node B [1].

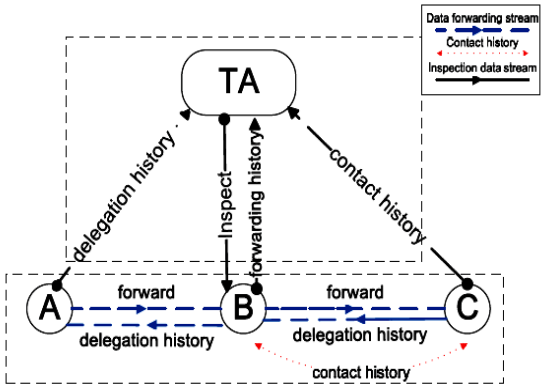

Figure 2: Evidence Generation and TA's Inspection [1].

To prevent the malicious users from providing fake evidences, TA should check the authenticity of each evidence. But due to this, it is observed that high

DOI 10.17148/IJARCCE.2016.52119

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

transmission and signature verification overhead occurs. To reduce this high verification cost, another scheme is introduced, i.e. Probabilistic Misbehavior Detection scheme [1].

The Li and Cao [3] proposed the scheme of packet dropping detection and routing misbehavior mitigation. A misbehaving node drops the received packets, if it has available buffers and it doesn't drop its own packets.
When two nodes meet, they generate the contact record. This contact record helps to show that at what time contact happened, which packets are in their buffers before data exchange and which packets they send or receive during data exchange. Also, the record includes the unique sequence number that each of them assigns for this contact. For integrity protection both the nodes sign a record. A node required to carry the record of previous contact and report it to its next contacted node. From these two reports, whether the packet is dropped by the node or not is detected [3].
For misreporting detection i.e. the nodes which reports false record, for each contact record, the node selects witness nodes and transmits record summery to them. The inconsistency caused by misreporting is detected by using summery part. The misreporting node is detected by witness node when the summaries of two inconsistent contact records will reach to witness node [3].
To reduce the routing misbehavior, reduce the number of packets sent to misbehaving node. The misreporting node should be included in blacklist. If node drops packets due to buffer overflow then the Forwarding Probability (FP) is maintained. The FP is based on nodes dropped, received and forwarded packets in recent contacts [3].

Li, Gao, Zhu and Cao presented the method for defending against flood attacks in disruption tolerant networks. DTNs utilize mobility of nodes and for data communication the opportunistic contacts among nodes are used. But due to limitations of network such as buffer space and contact opportunity, DTNs are vulnerable to flood attacks. For example, the attacker sends as many packets or packet replicas as possible to the network in order to overuse the limited network resources. To overcome this type of attacks, Packet Count Claim (P-claim) and Transmission Count Claim (T- claim) are used to detect packet flood attacks and replica flood attacks respectively. P- claim is generated by source and it is transmitted to later hops with packet. When contacted node receives this packet, it verifies the signature in p-claim, and checks the value of packet count of the source. If packet count is greater than rate limit then it discards the packet; otherwise it stores the packet and its P- claim. Source generates the T- claim and it appends to the packet. It is processed hop-by-hop. When the first hop receives this packet, it removes the T- claim, when it forwards the packet to next node, it appends a new T- claim to the packet. This process continues in a later hop. Each hop keeps the P- claim of source and T- claim of its previous hop to detect attacks. In single copy and multicopy routing, after forwarding packet for enough times, hop deletes its own copy of packet and will not forward packet again. To detect flood attacks in better manner, two nodes can exchange number of the recently collected P-claims and T- claims and check them for inconsistency[4].

Hur and Kang [5] proposed an attribute based secure data retrieval scheme for decentralized DTNs. The security is achieved using cipher text policy attribute based encryption (CP ABE).

The scalability and security is enhanced because each local authority issues partial personalized and attribute key components to user. The two party computation (2PC) protocols with central authority are performed. Each attribute key of a user can be updated individually and immediately [5].

Chen, Bao, Chang, Cho [6] presented the design of dynamic trust management protocol for secure routing in DTN. This protocol is validated by considering well behaved, selfish and malicious nodes. The trust management protocol considers the factors as trust composition, trust aggregation, trust formation and application level trust optimization designs. For trust composition design the quality of service and social trust properties are considered. The nodes trust level is in between 0 and 1. The protocol is validated using the simulation and it is compared with PRoPHET and Epidemic routing protocols.

III. COMPARISON

The overall discussion is summarized and compared in Table 1.

Table 1: Comparison of References

DTN Parameter	References					
	[1]	[2]	[3]	[4]	[5]	[6]
Misbehavior Detection	Yes	Yes	Yes	Yes	Yes	Yes
Misbehavior Reduction Technique	Yes	Yes	Yes	Yes	Yes	Yes
Defend Flood Attacks	Yes	Yes	No	Yes	No	Yes
Protocol Design	No	Yes	No	No	No	Yes
Trusted Authority	Yes	Yes	No	No	No	No
Trust Calculation	No	No	No	No	No	Yes

As indicated in Table 1, paper [1] provides the better security than others. This may be because as it provides the algorithm for probabilistic misbehavior detection. This algorithm reduces the high transmission and signature verification cost required for TA. The TA is a node which is trusted by the all other nodes in the network. The TA collects entire required history of related node and detects whether the particular node is misbehaved node or not. Hence, the TA plays important role in DTNs security. The node is said to be misbehaved in following situations:

DOI 10.17148/IJARCCE.2016.52119

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

a) If the node drops the packets or refuses to forward the data even when sufficient contacts are available.
b) The node forwards the packet but not following the routing protocol.
c) The node is agreed to forward the packet but fails to propagate enough number of copies [1].

The trust value of node is calculated by considering direct trust and indirect trust such as recommendations [6].

IV. IMPLEMENTATION DETAILS

For the implementation the Opportunistic Networking Environment (ONE) simulator is used. ONE is based on Java language. It is specifically designed for evaluation of routing in DTN. Based on various movement models, the specific scenarios are created. It supports for the routing protocols available for DTN such as Epidemic, PRoPHET, Spray and Wait, First Contact, Direct Delivery etc. The supported functions of ONE simulator are node movement modeling, node contacts, routing and message handling. The routing function is implemented by routing modules. The modules decide which message to forward over existing contacts. The event generators generate the messages. The messages are unicast, having single source and single destination. Simulation reports are collected through report generator. Each node has interface, persistent storage, movement, energy consumption and message routing. The nodes move according to movement models. The simulation scenarios are created by defining the parameters such as storage capacity, transmit range, bit rates etc [7].

Network Model
The network model is created with the DTN nodes. It contains two groups of nodes as p0 to p9 and c10. The node c10 will act as a TA as shown in figure 3.

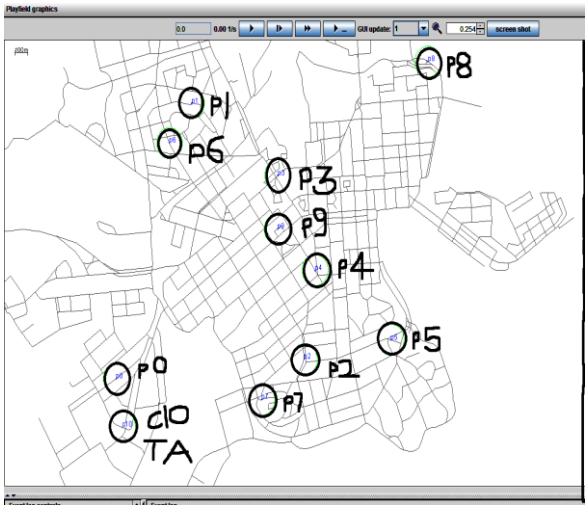

Figure 3: Network Model

The ONE Simulator routing setting used:
Interface= Bluetooth
Transmit Speed= 250k
Transmit Range= 100 M
Movement Model= Shortest Path Map Based Movement
Router= Epidemic
Buffer Size= 5M
GUI Underlay Image= helsinki_underlay.png

Experimented on AMD Phenom(tm) IIX4 B97 3.20 GHz processor and 8.00 GB RAM.

Contact History
In this type of history, whenever two nodes meet each other, the signature is generated using the nodes and timestamp. The algorithm used for signature is MD5.

As shown in figure 4, when the nodes c10 and p6 meet each other; to show the evidence of their meeting the signature is generated. In this way the contact history is created for all contacted nodes. This contact history is used by TA at the time of misbehavior detection.

ContactedNodes		Signature
c10	p6	7c19bb1711f8f84819c380577898b7a9
p1	c10	fcd3dee96404729b16a2c36486851e7d
p4	p0	f7a3855a5c695e44438c976fe12f7e18
c10	p1	42150c5e8d0a64bebcc090776f8118ef
p0	p7	add97a673501418e17f61093af5dd109
p8	c10	5bd226678aac6866777c7c6e8200dea1
c10	p8	836647c2b2842879829b076978d3714f

Figure 4: Contact History

Delegation History
When one node forwards the packet to next node then the next node gives the history back to its source node.

#fromHost	toHost	SigHashFrom	SigHashTo
p4	p8	d9752fea71698de6d0e5e4966d7ee3bf	d9752fea71698de6d0e5e4966d7ee3bf
p1	p0	92568d8477080374b96070b13dc4dd80	92568d8477080374b960700b13dc4dd80
p3	p1	a95e2942ec99f62609c54dbf0ec84a7e	a95e2942ec99f62609c54dbf0ec84a7e
p9	p1	4b8d25370a388cd8331785badbed1479	4b8d25370a388cd8331785badbed1479

Figure 5: Delegation History

As shown in figure 5, when the node p4 forwards the packet to p8 then node p4 gets delegate history. The delegation evidences are used to record number of routing tasks assigned from upstream nodes. When TA requires such history for misbehavior detection then the particular node gives the same to TA.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Forward History

The time when one node forwards the message to next node forward history is created.

fromHost	toHost	Signature
p4	p8	d9752fea71698de6d0e5e4966d7ee3bf
p1	p0	92568d8477080374b96070b13dc4dd80
p3	p1	a95e2942ec99f62609c54dbf0ec84a7e
p9	p1	4b8d25370a388cd8331785badbed1479
p4	p1	ce37dea46060de9dfe191a90386d8bbb
p3	p5	7fa3542114e810768a7f620dbb8ec934
p1	p3	1678a6e49ee6ed6e5de9adcb13aad967
p7	p3	32137abec06bc1e517f9ae709723fb07
p1	p3	aca77a35b02a07a9561253e0bdd46218

Figure 6: Forward History

As shown in figure 6, node p4 forwards the packet to node p8, at that time the signature is generated. This signature is used by TA at the time of misbehavior detection.

V. CASE EXAMPLES

Suppose TA has to check for node p1 if it misbehaved or not; TA collects the forward history from node p1, delegate history from node which sends packet to node p1 and contact history from set of contact list. The misbehaved conclusion can be drawn considerably in following cases:

Case 1: Packets are sent to p1from other nodes and if node p1 does not forward the packet to next node when sufficient contacts are available which satisfy the DTN routing protocol.
Case 2: Packets are sent to p1 from other nodes and p1 forwards packet to next node but next node not following routing protocol.
Case 3: Node p1 gets packets and it is agreed to forward it to next node but node p1 is fails to propagate enough number of copies in case of multicopy routing protocol.

To check node B, as shown in figure 2, when TA receives hash value as delegation history from node A and forward history from node B, if hash values do not match for a particular contact then node B is said to be misbehaved. The particular contact information is referred through contact history by TA.
The cases are derived according to the discussions made in section III. In these cases, to check node's behavior, there is need of transmission of records to TA and signature verification is required. But to check all the nodes in the network the overhead occurs in terms of transmission and signature verification. To reduce this overhead the probabilistic misbehavior detection algorithm is used. This algorithm helps to check particular node's behavior, TA launches the investigation with probability p_b. If that node passes investigation then TA pays compensation otherwise it will get the punishment [1].

VI. REMARK

In this paper, various trends of security in delay tolerant networks are studied and are compared. Due to misbehavior of node the performance of network affects and gives poor results. The secure routing in DTNs can be achieved by the use of efficient routing protocol i.e. which has high delivery ratio and low delay. The misbehavior is detected with low transmission and signature verification cost using the probabilistic misbehavior detection scheme using TA.

REFERENCES

[1] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in delay-Tolerant Networks," IEEE transactions on Parallel and Distributed systems, vol. 25, no. 1, pp.22-32, January 2014.
[2] Rongxing Lu, Xiaoding Lin, Haojin Zhu, Xuemin Shen, Bruno Preiss, "Pi: A Practical Incentive Protocol for Delay Tolerant networks," IEEE Transaction on wireless communications, vol. 9, no. 4, pp. 1483-1493, April 2010.
[3] Qinghua Li and Guohong Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2,pp. 664-675, Apr. 2012.
[4] Qinghua Li, Wei Gao, Sencun Zhu, Guohong Cao, " To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks," IEEE Transaction on Dependable and Secure Computing, vol.10, no. 3, pp. 168-182, May/June 2013.
[5] Junbeom Hur, Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption Tolerant Military Networks," IEEE/ACM Transactions on Networking, vol. 10, no. 1, pp. 16-26, February 2014.
[6] Ing-Ray Chen, Fenye Bao, Moon Jeong Chang, Jin-Hee Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," IEEE Transaction on Parallel and Distributed Systems, vol. 25, no. 5, pp. 1200-1210, May 2014.
[7] Ari Keranen, Jorg Ott, Teemu Karkkainen, " The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf. Simulation Tools and Techniques (SIMUTools '09), 2009.

DOI 10.17148/IJARCCE.2016.52119