A Trusted Misbehaviors Detection Scheme in Delay Tolerant Network

Sarawagya Singh
Student,
Department of Information Technology, Veltech
Dr. RR & Dr.SR Technical Unviversity

P. Prassenna
Assistant Professor,
Department of Information Technology, Veltech
Dr. RR & Dr. SR Technical Unviversity

ABSTRACT
Misbehavior of node represent a serious threat against routing in delay tolerant network. In this paper mainly focus to improve the packet loss during the transmission of packet one to another node and also deal with selfish and malicious node. In this paper introducing a periodically available trusted authority. TA judges any node in the network by collecting the history evidence from upstream and downstream node. TA could punish compensate the node based on its behaviors. Each node must pay deposit amount before it joins the networks, and the deposit will be paid after then node leave if there is no misbehaviors activity of node. In this paper also focus on security between the nodes in DTN. We introduced a secret key is generated, which is used to share the data. The secret key is automatically changed when the node joins a network and leaves a network based on fast randomized algorithm. So we can increase the level of security in delay tolerant network.

Keywords
Trusted authority, secret key, DTN, misbehavior

1. INTRODUCTION
In delay tolerant network Communication is possible even if end-to-end connectivity is never achievable. DTN Exploiting node's mobility and using store-carry-forward fashion. this is a new types of network are different from other kinds of networks. Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Disruption may exist because of the limits of wireless radio range, lack of mobile nodes, energy sources, attack, and noise. Delay tolerant network are those operating in mobile or extreme terrestrial domains, or planned networks in space. Delay tolerant network providing a convenient mode of communication for civilian and business purposes, DTNs networks are highly desirable for use in battle zones, relief efforts in remote area, and difficulty situations in disaster areas. In such cases, where no network infrastructures exist, DTNs network can provide a crucial mode of communication. Delay and disruption-tolerant networks (DTNs) are characterized by their lack of connectivity, resulting in a insufficiency of spontaneous end-to-end paths. A network of local networks supporting interoperability among them. An overlay on top of regional networks including the Internet accommodate long delays between and within regional networks and translate between regional network communication characteristics. The problems of DTNs can be affected by store-and-forward massage switching DTN routers need persistent storage for their queues because a communication link may not be available for a long time One node may send or receive data much faster or more reliably than the other node A message once transmitted may need to be retransmitted for some reasons. Assume communicating devices (nodes) in motion and or operation with limited power. When nodes must conserve power or preserve secrecy links are shut down -> intermittent connectivity network partition. On the Internet infrequent connectivity causes loss of data while DTNs disconnect delay with a store-and-forward approach. Network nodes may need to broadcast or connect during opportunistic contacts in which a sender and receiver make contact at an unscheduled time. The bundle layer a new protocol layer overlaid on top of heterogeneous region-specific lower layers with which application programs can communicate across multiple regions. Mainly nodes in DTNs are of two types which are more different from other networks.

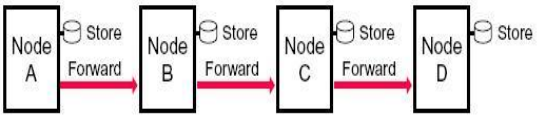

Fig: 1 a node store and forward in DTNs

Selfish nodes minimize their contributions to the network community and maximize their own gains by placing conniving nodes into the network community (to grab information). Malicious nodes attack proper network operations and do not consider their own gains. DTNs security protocols have to be more invulnerable and powerful to handle these types of nodes. Also the characteristics of DTNs and characteristics of mobile ad-hoc networks are distant which makes these security protocols ineligible for DTNs. DTN-specific security solutions are required. Therefore, traditionally security system is not suitable. Messages in DTNs are called as bundles. They traverse through Delay Tolerant Network bundle agents who partake in bundle communications to form the DTN store-and-forward overlay network. Misbehave mean that to behave badly or improperly. In the adhoc network that totally depend upon the each other node for exchange of information. Misbehave in network that node not perform its task in a proper way. In computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. in this paper mainly focus on gray hole attack,blackhole attack and wormhole attack .these attack are harmful attack against the DTN network.. Gray hole is a node that can transformation from behaving correctly to behaving like a black hole and it is literally an attacker and it will act as a normal node. black holes is an attack in the network where incoming or outgoing traffic is silently discarded (or "dropped") without informing the source that the data did not reach its intended recipient. worm hole attack are a network that mine information to another network, that is it get the data from one network replicate it into another network through tunnel . DTNs network are suffer from lack

of contemporaneous, end-to-end path High variation in network conditions, Difficulty to predict mobility, patterns Long feedback delay. Recently, there are quite a few proposal for misbehaviors detection in DTN, most of which are based on forwarding history verification (e.g., multi-layered credit, three-hop feedback transmission, or encounter ticket), which are costly in term of transmission overhead and verification cost. The basic idea of TA is to judge the node behavior based on the collected routing evidence. Before joining or leaving the node the contact to TA about the path before sending the packet one another node.

1.1. The Contribution of this Paper can be summarized as Follows

- Firstly, Trusted Authority (TA) to judge the node behavior based on the collected routing evidences. The trusted authority detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream node. Then TA could punish or compensate the node based on its behaviors. We assume that each node must pay a deposit amount before it joins the network, and the amount will be paid back after the node leaves if there is no misbehaviors activity of the node. TA could ensure the security of DTN routing at a reduced cost.
- Secondly, secret key is generated, which is used to share the data. the secret key is automatically changed when the node joins a network and leaves a network based on fast randomized algorithm. DTN is used to authorize the node when it wants to joins another node. So we can increase the level of security.
- Thirdly we introduce Randomized algorithms are specially useful when faced with a malicious "adversary" or attacker who deliberately tries to feed a bad input to the algorithm (see worst-case complexity and competitive analysis (online algorithm)such as in the Prisoner's dilemma.

2. RELATED WORK

In mobile adhoc networks, much work has been done to detect packet dropping and mitigate routing misbehavior. in adhoc networks used the neighbor node monitoring approach to detect the packet dropping. however for neighborhood monitoring rely on a connected link between the sender and its neighbour,which mostly likely will not exist in DTNs. a node may move away right after forwarding the packet to its neighbor, and thus cannot overhear if the neighbor forward the packet. In DTNs are not a proper connection between source and destination. So we cannot use ack approach before sending and receiving the packet.DTNs network mainly suffer from regular connectivity between the node. but in ad hoc network not suffer from connectivity. In adhoc network have regular connectivity between their node. in DTNs follow the store-carry forward mechanism and store the packet in node buffer until any node visible in transmission range.[1]proposed a social selfishness aware routing algorithm to allow user selfishness and provide better routing performance in efficient way. this approach deal with selfish node and also malicious node that not maximize their own benefit but to launch several attacks.[2] a secure multilayer credit-based incentive one of the most promising ways to address the selfishness issue and stimulate cooperation among selfish node in DTNs is using incentive scheme, which basically fall into two categories, reputation and credit-based scheme. Reputation based scheme rely on individual nodes to monitor neigh boring node traffic and keep track of each other. Where credit-based schemes introduce some form of virtual currency to regulate the packet forwarding relationships among different nodes. Our main focus on the detect the and avoid the packet loss during transmission from one node to other node and also provide security between the DTNs node .DTNs do not have the reliable link connection used in existing solution for node attacks.

3. PERLIMINARY

In this section, we formulate the network construction, request response based on trusted authority, data transmission, node construction based on secret key assignment, key changing based on node movement and design requirement.

3.1. Network Construction

In this network construction, first we have to construct a network which consists of ‘n’ number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, they can move across the network. All nodes are registered in the network and each node pay some amount during the registration process. Network is used to store all the Nodes information like Node Id and other information. Also network will monitor all the Nodes Communication for security purpose.

3.2. Trusted Model

There are mainly two types of node are found in the network. Misbehaving node and normal node. a misbehaving node are two types firstly, selfish node that enjoy the service provide by network that refuse to carry packet for other node and malicious node that drop the received packet even if it has available buffer. But it does not drop its own packet. a normal node may drop packet when its buffer overflow, but it follows our rule. Each packet has a certain life time and then expired packet should be lost no matter there is space or not. Such dropping can be easily identified if the expiration time of packet signed by the source. Trusted authority can be distinguished between the misbehaving and normal node on the basis of its forwarding history from upstream and downstream**.**

3.3. Request Response based on Trusted Authority

In this module, source node in network send data to destination means, before it sends the packet to trusted authority. That packet includes source node id, intermediate node id, destination node id, packet size and time. After receiving that packet trusted authority (TA) finds which node act as intermediate node. Then it sends request to all nodes for identifying intermediate node information. Based on that request each node sends the response to TA. Although TA auditing that information for identifying intermediate node trust worthiness using basic misbehavior detection algorithm.

3.4. Data Transmission

In this module, based on TA verification each node identifies the intermediate node behavior. Then source node securely transmits the data to destination node via honest intermediate nodes. Suppose node moves one network to another network means, network verifies if the node is honest or malicious based on probabilistic misbehavior detection algorithm. Then it refunds the amount based on node gentility. If the movable node is malicious means, network didn’t refund the amount.

3.5. Node Construction based on Secret Key Assignment

In this module, network act as the main resource for all node .for the node registration process, network assigns secret key for each node in network based on fast randomized algorithm. All node information stored in the network. Also the network will maintain node location information. Suppose attackers will entire in network mean based on secret key it easily identifies the attacker. Network verifies node secret key for security purpose.

3.6. Key Changing based on Node Movement

In this module, source node wants to move one network means, its private key also changed by network based on fast randomized algorithm. Same time once node move to another network means, existing network completely change the each node private key for security purpose. Suppose this source node hacks its previous network data means, it user their previous private key. But this private key. but this private key changed so it did not access previous network data.

3.7. Design Requirements

3.7.1. Distributed

We require that a network rule liable for the administration of the network is only periodically available and consequently ineffective of controlling the operation minutiae of the network.

3.7.2. Robust

We need a misbehavior detection scheme that could tolerate various forwarding decline caused by numerous network environments.

3.7.3. Scalability

We require a scheme that works regardless of the size and frequency network.

4. PROPOSED SCHEME

In this section we are introducing a secret key and a fast randomized algorithm. We know that a DTNs network have unique feature of intermittent connectivity, which makes routing absolutely distant from other kind of wireless networks. Since an end to end connection is hard to arrangement, store-carry and forward is used to transfer the packet to the destination.

Advantage

- Improved security.
- Less time consumption.
- No loss of data packet.
- Improved efficiency.
- Reduce the detection overhead adequately.
- Will reduce transportation overhead incurred by misbehavior detection and detect the malicious nodes effectively.

4.1. Secret Key

Secret key cryptography has been in use for thousands of years in a change of forms. Modern implementations normally take the form of algorithms which are completed by computer arrangement in hardware, firmware or software. The most of secret key algorithms are based on operations which can be performed very efficiently by digital computing systems. Traditionally, this technique employs algorithms in which the key that is used to encrypt the original plaintext message can be calculated from the key that is used to decrypt the cipher text message and inversely. It has been used primarily to provide confidentiality. In secret key cryptography (also called symmetric key cryptography), only single key is used to perform both the encryption and decryption functions. The encrypted message can be freely sent from one location to another through an insecure intermediate, such as the Internet or a dial link. As the name signified, secret key cryptography relies on both parties keeping the key secret. If this key is negotiated, the security offered by the encryption process is eliminated.

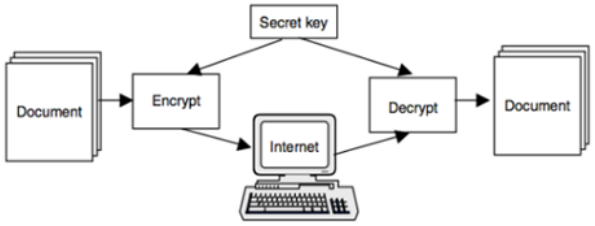

Fig: 2 secret key

Secret key cryptography has powerful limitations that can make it impractical as a stand-alone solution for securing electronic transactions, especially among large communities of users that may have no pre-established relationships. The most important limitation is that some means must be devised to securely distribute and key management manage the keys that are at the heart of the system**.**

4.1.1. Transmitting Over an Insecure Channel

It is generally impossible to avoid eavesdropping when transmitting information. For instance, a telephone conversation can be tapped, a letter can be interrupted, and a message transmitted on a LAN can be received by unauthorized stations. If you and I agree on a shared secret key then by using secret key cryptography we can send messages to one another on a medium that can be tapped, without worrying about hearers. All we need to do is for the sender to encrypt the messages and the receiver to decrypt them using the shared secret. An hearers will only see unintelligible data. This is the classic use of cryptography**.**

4.1.2. Secure Storage on Insecure Media

If I info I want to preserve but which I want to assure no one else can look at I have to be able to store the media where I am sure no one can get it. Between expert thieves and court orders, there are very few places that are actually secure, and none of these is hard. If I invent a key and encrypt the info using the key, I can store it any location and it is safe so long as I can remember the key. Of course, forgetting the key makes the data fully lost, so this must be used with great care**.**

4.1.3. Authentication

The term strong verification means that someone can prove knowledge of a secret without revealing it. Strong authentication is possible with cryptography. Strong authentication is particularly effective when two computers are trying to communicate over an insecure network.

4.2. A Fast Randomized Algorithm

This is an algorithm which gives excellent results when detect and verify on both source location as well as destination location networks and is much faster typically thousands of times faster than localized algorithms. It randomly provide a

key for each node in network It gives a new randomized algorithm for achieving consensus among asynchronous processes that communicate by monitoring for every node in the entire network based on node key. An algorithm that employs a degree of randomness as part of its logic. The algorithm consistently uses uniformly random bits as an auxiliary input to guide its behavior in the hope of obtaining good performance in the "average case" over all possible choices of random bits. Properly, the algorithm's performance will be a random variable determined by the random bits. thus either the executing time or the output (or both) are random variables**.** One has to analyze between algorithms that use the random input to reduce the expected running time or memory usage but always terminate with a correct result in a bounded amount of time and probabilistic algorithms. A fast randomized algorithms are approximated using a pseudorandom number generator in place of a true source of random bits. Such a performance may deviate from the expected theoretical behavior. A fast Randomized algorithms are particularly useful when faced with a malicious "adversary" or attacker who deliberately tries to feed a bad input to the algorithm.

4.2.1. Application of Algorithm

- It provide high security
- Easily identify the attacker
- Less time consuming process
- Avoid packet loss
- Quick data transmission

4.3. Trusted Authority

TA which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then, TA could punish or refund the node based on its behaviors. We assume that each node must pay a deposit amount before it joins the network and the deposit amount will be paid back after the node leaves if there is no misbehavior activity of the node. The basic misbehavior detection scheme to prevent malicious users from providing fake delegation/forwarding/ contact evidences. A should check the authenticity of each evidence by verifying the corresponding signatures which introduce a high transportation and signature verification overhead.

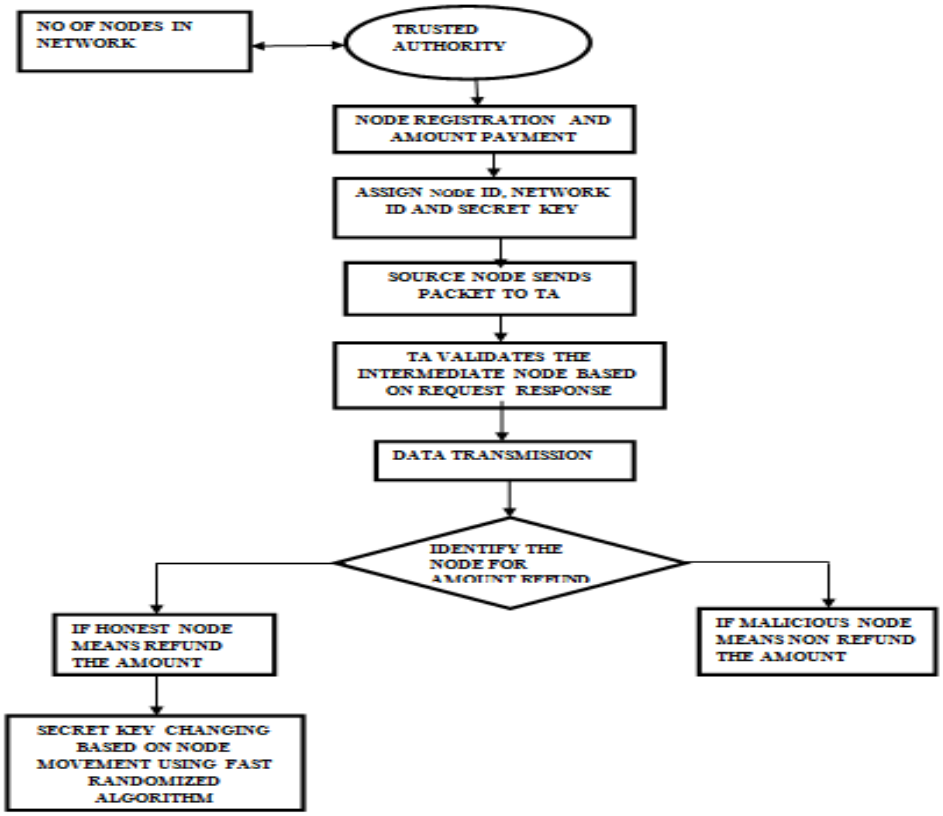

Fig: 4 Trusted Authority

5. FUTURE SCOPE

Presently work focus on the network like who suffer from lack of connectivity. in the future scope are mainly focus on the implement secret key mechanism other kind of wireless network for provide better service and security. So the use of this mechanism achieve high delivery rate of packet from source to destination**.**

6. CONCLUSION

In this paper, we mainly focus on the provide the security in the delay tolerant network node. So we introduced secret key mechanism and also focus on avoid the packet loss during the transmission in the network. Secret key provide is a secure way to pass the information from one node to another node. it achieve better performance by the use of secret key. The secret keys are automatically generated. So no one can guess the key of the node and it changing according to movement of node in the network.

7. REFERENCES

[1] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay- Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.

[2] SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks Haojin Zhu, *Member, IEEE*, Xiaodong Lin, *Member, IEEE*, Rongxing Lu, *Student Member, IEEE*, Yanfei Fan, and Xuemin (Sherman) Shen, *Fellow, IEEE* IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 8, OCTOBER 2009

[3] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858-3868, Oct. 2008.

[4] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.

[5] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom '00, 2000.

[6] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

[7] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM '09, 2009.

[8] W. Gao and G. Cao, "User-Centric Data Dissemination in Disruption-Tolerant Networks," Proc. IEEE INFOCOM '11, 2011.

[9] A. Keranen, J. Ott, and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf. Simulation Tools and Techniques (SIMUTools '09), 2009.

[10] A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks Haojin Zhu, Member, IEEE, Suguo Du, Zhaoyu Gao, Student Member, IEEE, Mianxiong Dong, Member, IEEE, and Zhenfu Cao, Senior Member, IEEE.

[11] http://en.wikipedia.org/wiki/Randomized_algorithm

[12] http://en.wikipedia.org/wiki/Key_(cryptography)