Volume-3, Issue-10, Oct-2014 • ISSN No 2277 - 8160

Research Paper ENGINEERING

A Secured Message Exchange Scheme in Post-Disaster Environment Using Delay Tolerant Network

CHANDRIMA CHAKRABARTI

Assistant Professor, CSE Dept. Narula Institute of Technology, Simultala, Agarpara, Kolkata-700109, West Bengal

ABSTRACT

Major Disasters turmoil human activity and disconnect communication services such as phones and Internet for weeks. To cope with such situations smart phone-based ad-hoc opportunistic network can be built to take rapid actions. Relief workers and victims can use these devices not only to produce information that can be incorporated into a shared situation awareness application, but also to validate the authenticity of information they use. In such sensational environment secure and immediate communication (or message exchange) among small groups and to remote monitoring system is quite important as there can be some malicious node intend to intercept and alter those sensitive data for the purpose of corruption. To implement secured message exchange, shared group keys can be assigned for encryption-decryption purposes to assure security. In this paper we can ensure secure communication among different components (called nodes) in Delay/Disaster Tolerant Network (DTN).The performance of the proposed scheme is evaluated using ONE simulator [8].

KEYWORDS : communication services; ad-hoc opportunistic network; situation awareness; secure and immediate communication; message exchange; malicious node; group keys; encryption-decryption; Delay/Disaster Tolerant Network

INTRODUCTION

Our Modern communication infrastructures that normally keep people connected and informed "on-the-go" have repeatedly proved to be unreliable and unavailable during and after large-scale disasters. Therefore to build up the minimal infrastructure for rescue operations will be prime need in that situation. Such communication network can be infrastructure less with typical mobility pattern and delay tolerant. One example of such an "infrastructure-less" network is described by the idea of hastily formed networks [1][2][9] built-up using the smart phones carried by the emergency responders. Relief workers from different agencies try to divide into different small groups based on different category of situational needs in timely manner [3]. If we consider medical team or military team as groups, they are not working in a particular area, rather they are scattered in different areas. Even group members may not know the actual location of its own group members. So, to build up proper communication within a group is very difficult. Also, in such sensational environment

secure and immediate group communication among small groups and to the remote monitoring system is very necessary as there can be some malicious node try to capture and modify those sensitive data for the purpose of dishonesty.

In this paper, our objective is to ensure fast and reliable delivery of messages in post-disaster communication network by avoiding the possibility of data modification by malicious nodes as far as possible. We propose a fast and secured Message Exchange Scheme with the help of different entities, called nodes, which are employed to deliver messages in sparsely connected network by using secured and shared group keys. We have simulated the scheme using ONE simulator [8].

RELATED WORK

In recent years, application of Delay Tolerant Network (DTN) in post disaster environment pays much attention of researchers. Huge amount of research have been done to assist group based data

exchange for the purpose of increasing reliability in a fragmented network like DTN.

In such opportunistic set-up, a node must decide whether to forward packets to an encounter node based on contact history [5][7]. But in that case authors [5][7] are not considering question of data integrity, which may be hampered. In [4] F. Li et. al. proposed an enhanced group-based routing protocol for delay tolerant networks, in which the relay node is selected based on social group information obtained from both historical encounters. We feel that in disaster environment it is not possible to meet each group members within a zone, because they are scattered everywhere. So, encounter metric does not work always. In [6] R. Zhou et. al. discussed about their Group Based Epidemic Routing (G-Epidemic) for propagating group information with the help of group member. But we observed that in this scheme delay in data delivery is huge as in a fragile environment like DTN, nodes contacts are opportunistic in nature. So, a node needs to wait for a long time to find its own group member or friend. At the same time authors in [6] are not considered secured delivery of data.

Inspired by the existing research works, we aim to design a secured message exchange scheme using shared group key in a post-disaster communication scenario. In this paper, we have tried to secure the data using shared group key which is available to group members only for encryption- decryption purposes.

SYSTEM MODEL

In post-disaster environment volunteers who are working in group, will choose some buildings, schools as local shelter for temporary residence of victims after rescued them. Total no. of groups, type of groups, no. of people allocated to each group may be varied based on the disaster type and situation. Shelters can also be used as the local office of different volunteer groups, temporary storage of needs like rice, dry foods, medicine etc for survivals. Updated information of all shelters (information like actual situation of the areas, demand of each shelter, no. of victims) will be forwarded time to time to the Control Station node, which is situated in nearby city.

Now, from each shelter, volunteer groups will be divided into lesser no. of groups and worked in different locations; but before that, each volunteer group needs to register at shelter and get shared secret key for ensuring secured message exchange.

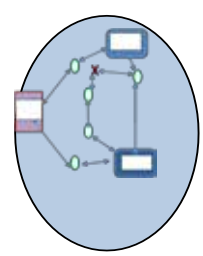
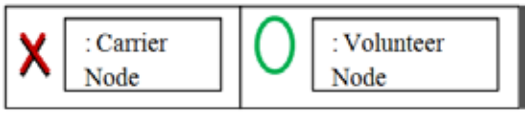


Fig.1. Representation of Different Nodes in the Proposed System Model
Where CS : Control Station Node,



As in Fig. 1, Control Station node controls all the shelter nodes and gets up-to-date information from them. Volunteer nodes are responsible for forwarding messages securely either directly in one hop or via multi-hop volunteer nodes. Volunteer nodes may sometimes get the help of carrier nodes, which are used in group communication for delivering messages time to time.

Data forwarding using volunteer node:
Suppose, a volunteer node wants to send the message to its group member node, first it encrypts

the message with shared group key. Then after searching neighbor table, if it finds the destination node is in its 1 hop neighbor, then delivers it directly.

When a volunteer node within a particular zone needs to send some message to other node, first consults its neighbor node table as below:

TABLE - 1
EXAMPLE OF NEIGHBOR TABLE OF A VOLUNTEER NODE

Node idt	Group id	Location
s1 (shelter node)		(x,y)
v11s1 (volunteer node of group1)	g1	(x11,y11)
v12s1 (volunteer node of group1)	g1	(x14,y14)
v21s1 (volunteer node of group2)	g2	(x12,y12)
v31s1 (volunteer node of group3)	g3	(x13,y13)
cn11 (carrier node1)		(x1,y1)

But if it can't find it in the neighbor table, then it needs help from carrier node. If that particular volunteer node finds any carrier node within its vicinity, it forwards the message to that carrier node. As using carrier node a message can be forwarded fast.

In this paper we assume that carrier nodes are responsible for forwarding messages to volunteer nodes only. For delivering messages to shelter nodes, volunteer nodes are solely liable.

Communication with Shelter node and Control Station node:
If shelter node has to send some message to the affected zone or vice versa which is not specific for a group, shelter node can broadcast the message. If any volunteer group has to send some message from shelter to the disaster affected zone or vice versa, then volunteer group or node need to encrypt the message using shared group key. After collecting all information from disaster struck zone, at shelter, different volunteer groups will decrypt those information and try to generalize the overall

information. These volunteer groups (those who reside at shelter) will again encrypt that information using shared group key and send it towards Control Station node via single or multi-hop volunteer nodes.

Using this scheme Control Station (CS) node gets updated information of needs from different shelter nodes. We assume CS node has the authority to get access of all shared group keys. Control Station node allocates relief materials for meeting the needs of different shelters and sends them to the shelter nodes via volunteer nodes as well.

SIMULATION
We have implemented our scheme using Opportunistic Network Environment (ONE) simulator [8]. The nodes are positioned on default map. The details of our simulation parameters are shown in table2:

TABLE - 2
PARAMETERS USED FOR SIMULATION

No. of groups volunteer nodes	3
No. of Volunteer nodes (Mobile)	Varies from 50 to 200
No. of Shelter nodes (Stationary)	3
No. of Control Station nodes (Stationary)	1
No. of Carrier nodes (Mobile)	10% of total number of volunteer
Speed of Volunteer node	0.5 m/s -1.5 m/s
Speed of Carrier node	1.5 m/s – 5.5 m/s
Transmission range	10 m
Transmission speed	2 Mbps
Buffer size of volunteer node	5 MB
Buffer size of carrier node	500 MB
Message size	500 kB- 1MB
Movement Model	Shortest Path Map Based Movement
Routing Protocol	Spray and Wait Routing
Simulation time	12 Hours

The performance of our proposed scheme is evaluated and compared with the ONE [8] default non-secured environment where encryption- decryption and carrier nodes are not used. For comparison purposes we used packet delivery probability as the parameter.

Delivery Probability = No. of Packets Delivered / No. of Packets Created

From Fig. 2, it is evident that the delivery probability improves in our proposed scheme compared to the ONE default non-secured environment [8].

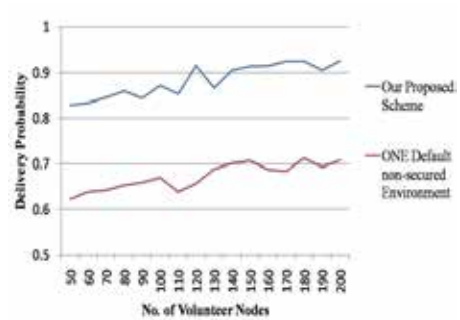


Fig. 1. Simulation result of No. of Volunteer node vs. Delivery Probability with our proposed scheme and ONE default non-secured environment; our proposed scheme gives better result

CONCLUSION AND FUTURE WORK
This paper presents a secured message exchanged scheme using shared group key for data encryption-decryption by the group members and

carrier nodes for fast and reliable data dissemination. It is a novel approach as

i) We have tried to achieve data integrity, content of data remains intact.
ii) Using our scheme, unnecessary dropping, non-forwarding, colluding attacks can be avoided.

Here we assumed that carrier nodes are authorized and reliable. But if this situation varies, then our system will not give better delivery. In near future we will try to solve this issue in larger perspective.

REFERENCES

[1]Asplund, M., Tehrani, S.N., Sigholm, J. : Emerging Information Infrastructures: Cooperation in Disasters, Critical Information Infrastructure Security: Third International Workshop, CRITIS 2008, Rome, Italy, October13-15, 2008. | [2]The audit of disaster-related aid(Main), ISSAI 5520, http://eca.europa.eu/portal/pls/portal/docs/1 /22006772.PDF [3]Chakrabarti, C., Banerjee, A., Roy, S. : An Observer- based Distributed Scheme for Selfish- Node Detection in a Post-disaster Communication Environment using Delay Tolerant Network, 2014 IEEE International Conference on Applications and Innovations in Mobile Computing, pp. | 151-156, 2014 | [4] Li, F., Zhang, C., Gao, Z., Zhao, L., and Wang, Y.: Social Feature Enhanced Group-based Routing for Wireless Delay Tolerant Networks, Mobile Ad-hoc and Sensor Networks (MSN), 2012 Eighth IEEE International Conference14-16 Dec. 2012 | [5]Wu, J., Xiao, M., Huang, L.: Homing Spread: Community Home-based Multi-copy Routing in Mobile Social Networks, INFOCOM, 2013 Proceedings IEEE [6]Zhou, R., Cao, Y., Jin, J., Zhu, D., : Group Based Epidemic Routing for Delay and Tolerant networks, Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference | 23-25 Sept. 2010 | [7]Chang, J.W., Chen, C. : CROP: Community-Relevance- Based Opportunistic Routing in Delay Tolerant Networks, | 2013 IEEE Wireless Communications and Networking | Conference (WCNC) | [8]The Opportunistic Network Environment simulator (The | ONE), http://www.netlab.tkk.fi/tutkimus/dtn/theone /Ver. | 1.4.0, 2010 | [9] Chakrabarti, C., Chaki, R.: Improved Cluster based Route Discovery Algorithm for Ad-hoc Networks, IEEE Proc. ICCIA 2011 Pages- 1-4. |