ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Reliable Route Discovery and Secure Routing In Delay Tolerant Network

Asha S S[1], Kiran Babu T S [2]

M.Tech (CNE), Department of Computer Science, CMR Institute of Technology, Bangalore, Karnataka, India[1]

Assistant Professor, Department of Computer Science, CMR Institute of Technology, Bangalore, Karnataka, India[2]

ABSTRACT: Delay tolerant network (DTN) is one of the key areas in wireless communication. Characteristics of delay tolerant network include intermittent connectivity, discontinuous connection from source to destination. It is an approach to computer network architecture that seeks to address the technical issues of heterogeneous network architecture which lack continuous network connection. This layer handles long delays, disconnectivity and high lose rate due to disruption. Data will be stored in persistent storage on DTN device and it will be forwarded to other node where the link is available. Main objective of this paper is to overcome the security attacks in delay tolerant network and also to improve the link quality of the nodes. Since the nodes in the wireless sensor network will be subject to different attacks, different measures are taken to overcome the attacks and to reduce the delay. As a result the packet delivery ratio is increased and hacking probability is reduced and network lifetime of node so that link quality will be more

KEYWORDS: Delay Tolerant Network, Malicious Node, Blowfish Algorithm.

I. INTRODUCTION

Delay tolerant network is general purpose network architecture. Different design themes are considered while designing the DTN. They are leverage storage resources to avoid consuming network bandwidth, handle intermittency at multiple points in the network and mechanism to handle network outrages. Delay tolerant networks are characterized by their lack of connectivity resulting in lack of instantaneous end to end path. Delay tolerant network adopts store and forward mechanism to routing. Interoperability of regional networks is supported by delay tolerant network.Characteristics of delay tolerant network include intermittent connectivity, discontinuous connection from source to destination. A DTN environment with no centralized environment is considered. Nodes will communicate through multiple hops. DTN includes VANET, ,MANET, Wireless Sensor Nodes etc. Here in this project wireless sensor nodes are used. These sensor nodes may include normal nodes and it includes some misbehaving nodes such as malicious nodes. Malicious nodes performs some attacks such as self-promoting attacks, bad-mouthing attacks.

II. RELATED WORK

An Opportunistic On Routing Protocols and Persisting Challenges in Delay-Tolerant Networking[1] In this paper they have mentioned different challenges faced by delay tolerant network and how to overcome those challenges. It is mentioned that delay tolerant networks network connectivity is prone to errors and disruptions. The network topology may be dynamically changing. Different routing protocols can be used for routing purpose. The routing protocols have to use store and forward mechanism. Bundle protocol is one such routing protocol.

Custody Transfer for Reliable Delivery in Delay Tolerant Network[3], in this paper it is given about the custody transfer mechanism used in delay tolerant network. In internet architecture, end to end delivery of packets takes place in case of failure of network connectivity. But in case of delay tolerant network instead of end to end delivery of packets or messages it adopts the method of hop by hop message delivery of packets which is more reliable and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

efficient. Security can be provided end to end, path to path etc. IPSEC protocol is used as network layer security protocol.

III. SYSTEM MODEL

We consider a DTN environment with no centralized trusted authority. Nodes communicate through multiple hops .When a node encounters another node, they exchange encounter histories certified by encounter tickets so as to prevent black hole attacks to DTN routing. We differentiate socially selfish nodes from malicious nodes. A selfish node acts for its own interests including interests to its friends, groups, or communities. So it may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good social ties with the source, current carrier or destination node.

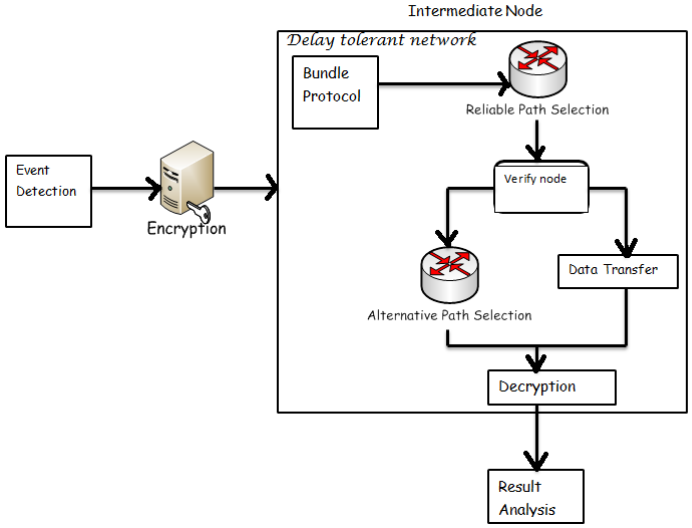


Figure 1: Architecture of the proposed system

Here to voting based routing algorithm is used for routing. Nodes are selected based on communication range, distance covered and energy consumed. By selecting the neighbour nodes which are present in the communication range the energy consumed will be reduced and the link quality will be increased. Blowfish algorithm is used to encrypt the data.

(a) Detection of malicious Nodes

Malicious nodes are the one which performs attacks like self-promoting attack and bad-mouthing attack. In this project sensor nodes are used. The primary function of wireless sensor networks is to gather sensor data from the monitored area. Due to faults or malicious nodes, however, the sensor data collected or reported might be wrong. Hence it is important to detect events in the presence of wrong sensor readings and misleading reports.Malicious nodes are modelled as faulty nodes behaving intelligently to lead to an incorrect decision or energy depletion without being easily detected. Here malicious nodes are detected based on some parameters. These parameters are communication range, distance and energy consumed. Initially these parameters are set to every node. If any node sets back in the threshold values then it will be detected as a malicious node.

(b) Blowfish encryption algorithm

Blowfish algorithm is used for encryption and decryption purpose. It is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. It was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

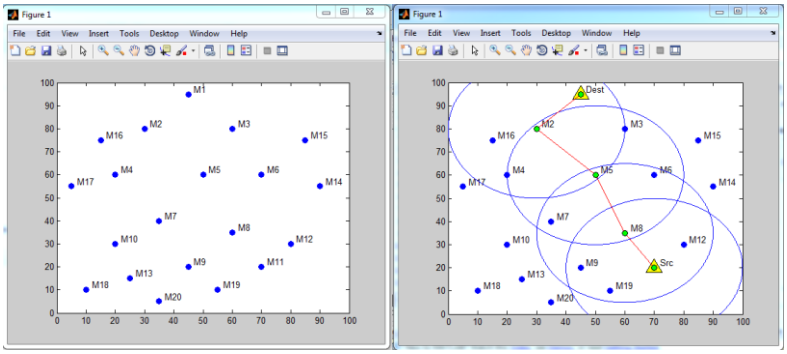
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

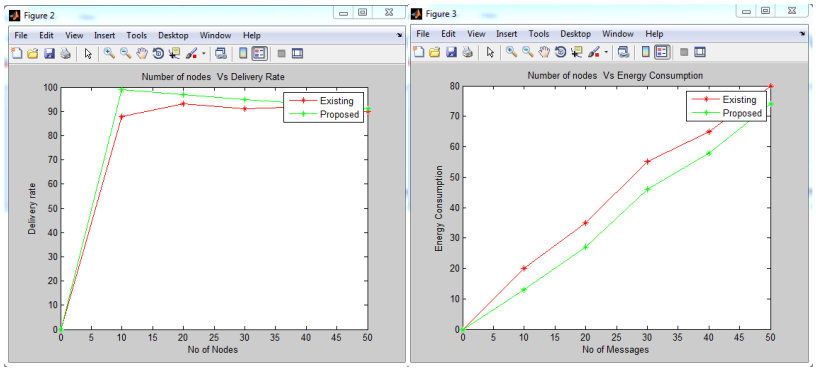
Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

IV. EXPERIMENTAL RESULTS

Figure 2 .The following diagrams (a) Initially some nodes are created randomly. After that source and destination nodes are selected.Once the nodes are selected then the route is established using voting based routing algorithm. Data is encrypted then the encrypted data will be sent along the route established. (c),(d) shows the simulation results of the proposed system, graph shows that the packet delivery rate will be more if the number of nodes is more.



(a) (b)



(c) (d)

V. CONCLUSION

In this paper we designed an architecture for secure routing of the data in delay tolerant network using sensor nodes. Malicious nodes are detected based on few parameters and they are communication range, distance and energy. For encryption blowfish algorithm is used.Future work may be done on this paper. Some other algorithms can be used for encryption and also for the detection of malicious nodes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networking," Proc. IEEE INFOCOM, pp. 1-11, Apr. 2006.
[2] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture,"RFC 4838, IETF, 2007.
[3] I.R. Chen, F. Bao, M. Chang, and J.H. Cho, "Supplemental Material for 'Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing'," IEEE Trans. Parallel and Distributed Systems, 2013.
[4] I.R. Chen and T.H. Hsi, "Performance Analysis of Admission Control Algorithms Based on Reward Optimization for Real-Time Multimedia Servers," Performance Evaluation, vol. 33, no. 2, pp. 89-112, 1998.
[5] S.T. Cheng, C.M. Chen, and I.R. Chen, "Dynamic Quota-Based Admission Control with Sub-Rating in Multimedia Servers," Multimedia Systems, vol. 8, no. 2, pp. 83-91, 2000.
[6] S.T. Cheng, C.M. Chen, and I.R. Chen, "Performance Evaluation of an Admission Control Algorithm: Dynamic Threshold with Negotiation," Performance Evaluation, vol. 52, no. 1, pp. 1- 13, 2003.
[7] J.H. Cho, A. Swami, and I.R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Comm. Surveys & Tutorials, vol. 13, no. 4, pp. 562-583, Fourth Quarter 2011.
[8] E.M. Daly and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," IEEE Trans. Mobile Computing, vol. 8, no. 5, pp. 606-621, May 2009.
[9] M.K. Denko, T. Sun, and I. Woungang, "Trust Management in Ubiquitous Computing: A Bayesian Approach," Computer Comm., vol. 34, no. 3, pp. 398-406, 2011.
[10] V. Jacobson, D.K. Smetters, J.D. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking Named Content," Comm. ACM, vol. 55, no. 1, pp. 117-124, 2012.
[11] A. Jøsang and R. Ismail, "The Beta Reputation System," Proc. Bled Electronic Commerce Conf., pp. 1-14, June 2002.
[12] S. Kosta, A. Mei, and J. Stefa, "Small World in Motion (SWIM): Modeling Communities in Ad-Hoc Mobile Networking," Proc. Seventh IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks, June 2010.