IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 13, Issue 2, Ver. I (Mar. - Apr. 2018), PP 21-24
www.iosrjournals.org

Improved Data Delivery Ratio with Less Transmission Delay in ICWN

Shweta Premchand Pitambare[1], Prof. V.V. Yerigeri [2]
[1](PG Department, M.B.E.Society's College of Engineering, Ambajogai India)
[2](PG Department, M.B.E.Society's College of Engineering, Ambajogai India)

Abstract: *Improved version of DTN (Delay tollerent network) is ICWN. In ICWN (intermittently connected wireless networks) nodes are not directly connected to each other instead it is connected randomly according to the relationship between the neighbour nodes. So the data forwarding in ICWN with less latency and high data delivery rate is very difficult. In this paper we obtain the improved data delivery ratio with increased speed and high QOP (Quality of protection) by using BPSK modulation. To forward data in ICWN, the process based and relationship based credibility is considered for finding the neighbour nodes. The numerical result shows the comparison between the conventional techniques (PROPHET and Trust threshold) and QOP-DF (Quality of protection data forwarding) technique. Numerical result shows the reliable data transmission with improved QOP, reduction of latency, and increased data delivery ratio.*

Keywords: *DTN(Delay tollerent network), ICWN(intermittently connected wireless networks), QOP(quality of protection)*

Date of Submission: 23-02-2018 Date of acceptance: 12-03-2018

I. Introduction

ICWN avoids establishing the end to end path; it is different from the mobile ad hoc networks (MANETs). Store-carry-forward method is used in the ICWN network to send the data hop by hop due to that the data forwarding in highly dynamic and intermittently connected network is possible. Internet research task force proposed the ICWN as an emerging mobile network [1]. Routing protocols are defined in DTN based on the information used. In ICWN for better quality of experience (QOE) for users, the data delivery is more challenging. Subjective experience of users during the service process is the QOE [2]-[3]. In traditional internet model instead of assuming end to end path, messages are exchanged opportunistically when encounter happens between nodes [4]. A probabilistic misbehavior detection scheme in DTN routing for efficient trust establishment, which is called as iTrust is proposed in [5]. A conceptual framework for security evaluation with some practical consideration is presented in [6]. It is based on security requirement and evidence collection. Opportunistic data forwarding is explained in which the intermediate nodes will store-carry and forward messages in opportunistic way. It uses a SMART scheme to forward the data to provide motive to selfish nodes. For data forwarding it uses native multilayer coin scheme. When node send the data, the node will lose credit to the network because other node gain a cost to forward the data [7]. Private key signatures and encounter tags are used by the nodes to verify the encounter history information due to that credibility and service ability is estimated [9]. A positive forwarding message (PFM) is used to verify the forwarding behavior [10].

In this paper we are considering the general data forwarding process in ICWN. Process based and relationship based credibility is evaluated according to the encounter history information. Data forwarding in ICWN is explained briefly. Numerical analysis shows the comparison between the proposed technique and the conventional technique in ICWN for data forwarding. Numerical results shows the proposed technique is having high data delivery ratio under different proportion of malicious nodes and less average transmission delay under different proportion of malicious nodes. As the number of malicious nodes will increase, the data delivery is crucial but as we used the BPSK modulation for data forwarding, the improved data delivery ratio is obtained.

II. General Data Forwarding In ICWN

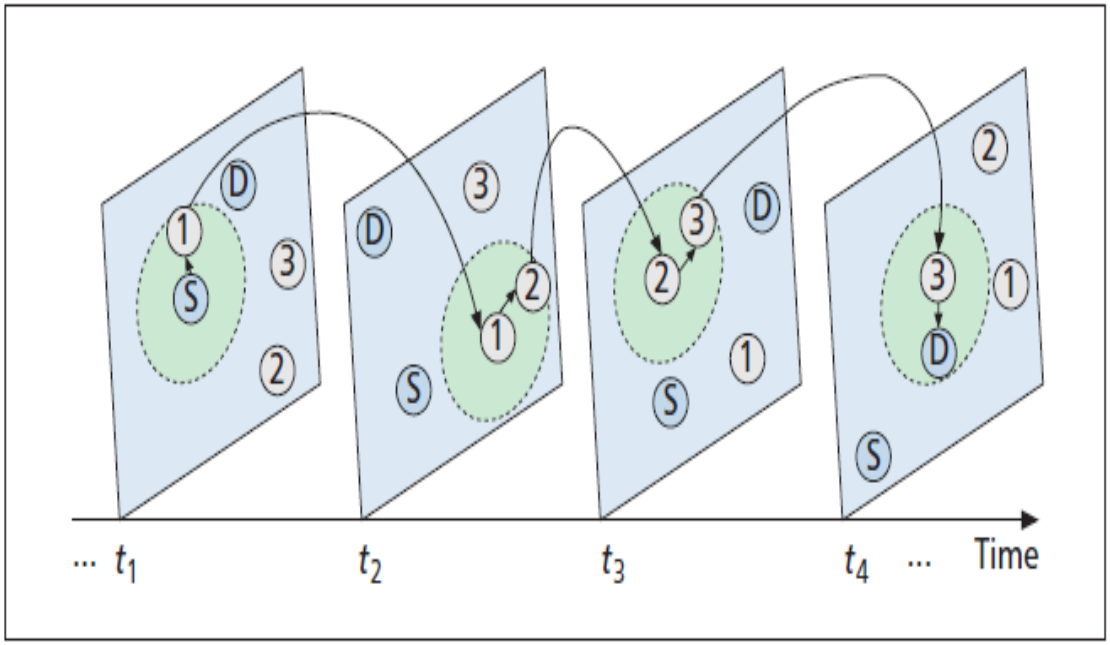

Fig. 1 : General data forwarding in ICWN

Fig. 1 illustrates the data forwarding in the intermittently connected wireless networks. There will be no direct path from the source node to destination node at a given time. To send the data from the source node to destination node, the intermediate node will store and carry data to the next node. To send the data from one node to other node, nearest node which is having more signal strength is calculated and forwarded to that node. Data transmission in the ICWN in the presence of malicious nodes, the social relationship between the nodes is calculated that means which node is having high signal strength and which is nearer to the source node. After the connection established between the nodes, the neighbour list is updated according to the signal strength and nearest node. The data carrying node checks whether the encountered node is the destination node or not if it is destination node, it will deliver the data to the node otherwise again it will relationship based and process based credibility is calculated, according to that the neighbour list is updated. To forward the data from one node to other node BPSK modulation technique is used.

The product of the average connection duration $dur_i^j(t)/t$ and the encounter times $n_i^j(t)$ is the encounter strength between the node i and j, where the total connection duration is $dur_i^j(t)$. The data exchange between two nodes which are having no mutual neighbour, the node relationship strength $b_{i,j}(t)$ is defined as $e^{\propto -1}$, where

$$\alpha = \left[dur_i^j(t) \Big/ \sum_{k=1}^{n_i^N(t)} dur_i^k(t) \right] \cdot \frac{|\Gamma(i) \cap \Gamma(j)|}{|\Gamma(i)|} \tag{1}$$

and $n_i^N(t)$ is the number of encountered nodes. The relationship strength is zero when the two nodes never meet and have no mutual neighbours.

According to the historical node behavior node credibility can be evaluated. The node credibility is divided into two parts process based credibility and relationship based credibility. Relationship based credibility is related to social characteristic such as network topology and node trajectory. Negative forwarding and malicious discarding of data is measured by the process based credibility. Bye using BPSK technique with increase in malicious nodes average transmission delay is decreased and the data delivery ratio is also increased. After receiving the data, the acknowledgement will be send due to that the speed of the data transmission is improved.

III. Evaluation Of Node Credibility

Node credibility effectively evaluated if its value is defined as the variable between [0,1]. Distrust is indicated by 0, 0.5 is for unknown trust status and 1 is for full trust. $T_{i,j}(t)$ is the credibility value of node j at time t.

$$T_{i,j} = \beta . T_{i,j}^{beh}(t) + (1 - \beta) \cdot T_{i,j}^{s}(t) \quad (2)$$

Where $T_{i,j}^{beh}(t)$ and $T_{i,j}^{s}(t)$ is the process based and relationship based credibility respectively.

A hop by hop feedback mechanism is used for the successful data forwarding in process based credibility evaluation. As well as the acknowledgement is used for the successful delivery of data. Exponential function and arc tangent function is used for calculation of process based credibility, which are given as $1/\pi$ arctan $r_{k,m}$ and $(1/2)e^{-f_{k,m}}$. Node trajectory and network topology is used to calculate the relationship based credibility, which measures the trust relationship based on node similarity. The high QOE is obtained in closely related nodes with tight social relationship. Relationship closeness and service similarity is used to calculate the relationship based credibility, where service similarity shows the two nodes providing service to same node.

IV. Numerical Results

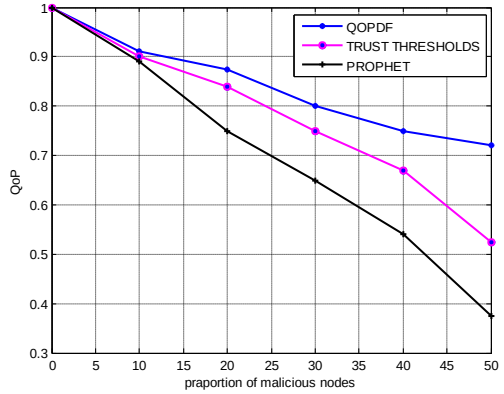

Fig. 2: The QOP under different proportions of malicious nodes

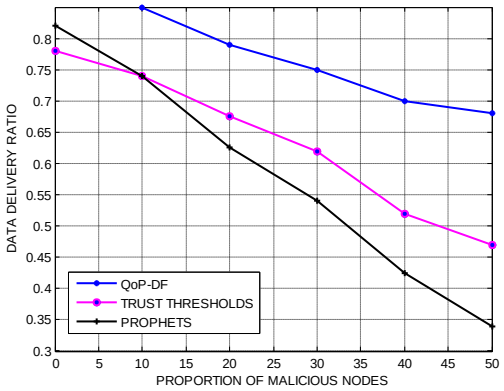

Fig. 3: Data delivery ratio under different proportions of malicious nodes.

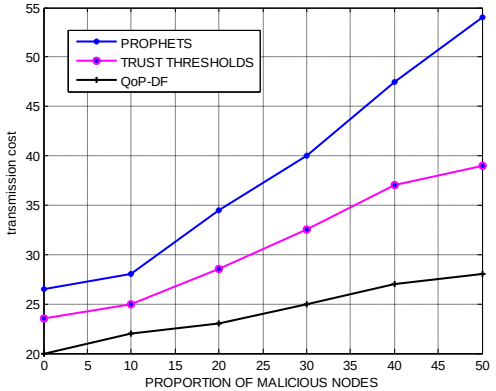

Fig. 4: Transmission cost under different proportion of malicious nodes.

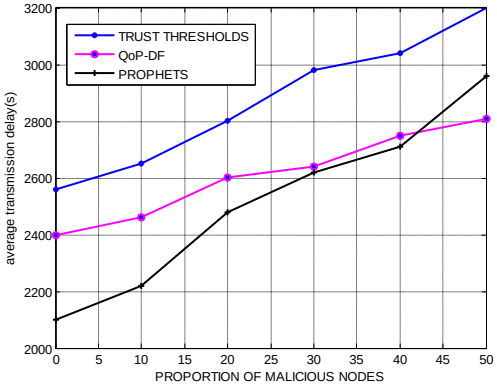

Fig. 5: Average transmission delay under Different proportion of malicious nodes

Fig. 2 shows the QOP under different proportion of malicious nodes. As the number of malicious nodes increases, the QOP will be reduced. As compared to the conventional technique, the proposed scheme provides the better QOP under more number of malicious nodes. Fig. 3 gives the analysis of the data delivery ratio with respect to the malicious nodes. The data delivery ratio of the proposed system is more as compared to the conventional techniques used for data forwarding in ICWN. Fig. 4 indicates the transmission cost required for the data transmission under different proportion of malicious nodes. Graph shows that transmission cost of the QOP-DF is very less as compared to other techniques. Fig. 5 gives the latency required for the conventional

techniques and the proposed techniques. It is clear from the graph that the transmission delay required for QOP-DF is very less as compared to other.

We used the BPSK technique instead of using the relay transmission for data transmission so that we obtain the high data delivery ratio and less transmission delay based on the results of Fig. 3 and 5.

V. Conclusion

The existence of malicious nodes greatly decreases the network QOP, utilization of resources, data delivery ratio. Bye using the social relationship between the nodes the data is forwarded in ICWN. To forward the data we have used the process based and relationship based credibility. By using the values obtained in the credibility evaluation, the data is transmitted by using BPSK modulation technique. Due to that we obtained the high speed data transmission with more data delivery ratio. The improved data delivery ratio is obtained in this paper also we reduced the average transmission delay under the effect of malicious nodes. The QOP for the data forwarding is also maintained so that this method is good for secure communication with high speed. Transmission cost is also less as compared to the conventional technique.

Acknowledgements

We convey our sincere thanks to the Principal Dr. B. I. Khadakbhavi, Dean of P. G. Department Dr. B. M. Patil and staff of MBES's College of Engineering, Ambajogai for help in carrying out this research work at the institute.

References

[1] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, *"Disruption- Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges." IEEE Commun. Surveys & Tutorials, vol. 14, no. 2, 2012, pp. 607–40.*

[2] Z. Zhang, *"Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks:Overview and Challenges." IEEE Commun. Surveys & Tutorials, vol. 8, no. 1, 2006, pp. 24–37.*

[3] S.N. Foley et al., *"Multilevel Security and Quality of Protection,"* Proc. First Workshop on Quality of Protection, Como, Italy, Sept. 2005.

[4] V. S. Mota, F. D. Cunha, and D. F. Macedo, *"Protocols, Mobility Models and Tools In Opportunistic Networks: A Survey," Computer Commun.*, vol. 48, no. 4, 2014, pp. 5–19.

[5] H. J. Zhu et al., *"A Probabilistic Misbehaviour Detection Scheme toward Efficient Trust Establishment in Delay- Tolerant Networks," IEEE Trans. Parallel Distrib Sys., vol. 25, no. 1, 2014, pp. 22–32.*

[6] R. Savola and J. Roning, *"Towards Security Evaluation Based on Evidence Collection,"* Proc. Third Int'l Conf. Fuzzy Systems and Knowledge Discovery,Xi'an, China, Sept. 24–28, 2006, pp. 1178–81.

[7] H. J. Zhu et al., *"SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans.* Vehic. Tech., vol. 58, no. 8, 2009, pp. 4628 39.

[8] Chen et al., *"Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," IEEE Trans.* Parallel Distrib. Sys., vol. 25, no. 5, 2013, pp. 1200–10.

[9] F. Li, J. Wu, and Srinivasan A, *"Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets,"* Proc. *IEEE INFOCOM* '09, 2009, pp. 2428–36.

[10] N. Li and S. K. Das, *"A Trust-Based Framework for Data Forwarding in Opportunistic Networks,"* Ad Hoc Networks, vol. 11, no. 4, 2011, pp. 1497–1509.

[11] Dapeng wu, Hongpei zhang, Honggang wang, Chonggang wang, Ruyan wang, And Yi Xie ,"*Quality Of protection driven data forwarding for intermittently connected wireless network*" IEEE Wireless Communications

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

Shweta Premchand Pitambare "Improved Data Delivery Ratio with Less Transmission Delay in ICWN." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 13.1 (2018): 21-24.