Disjoint Multipath Based Secure Routing in Opportunistic Networks

Sanjay K. Dhurandher[1], Jagdeep Singh[2], Isaac Woungang[3], Joel J. P. C. Rodrigues[4,5]

[1] Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
[2] Division of Information Technology, Netaji Subhas Institute of Technology, University of Delhi, India
[3] Department of Computer Science, Ryerson University, Canada
[4] Federal University of Piau'i (UFPI), Brazil
[5] Instituto de Telecomunicações, Portugal
dhurandher@gmail.com, jagdeepknit@gmail.com, iwoungan@scs.ryerson.ca, joeljr@ieee.org

Abstract

Opportunistic Networks (OppNets) are composed of wireless nodes opportunistically communicating with each other. These networks are designed to operate in a challenging environment characterized by high delay, intermittent connectivity, and no-guarantee of fixed path between the sender and destination nodes. One of the most vital issues in designing such a network is the security of the messages flowing in it. This paper proposes a new method called Disjoint Multipath based Secure Routing in Opportunistic Networks, called as D-MUST, which relays the message to the destination through four disjoint paths; each applying a soft-encryption technique to prevent message fabrication attacks. Simulations are conducted using the *HAGGLE INFOCOM 2006* real mobility data traces, showing that when time-to-live is varied, (1) the proposed D-MUST scheme outperforms RSASec by 15.05%, 8.4%, 5.81% 2.16% respectively in terms of delivery probability, hop count, messages dropped and average latency; (2) it also outperforms SHBPR by 16.17%, 9.2%, 6.85%, 3.95% respectively in terms of delivery probability, hop count, messages dropped and average latency.

Keywords: Opportunistic Networks (OppNets), Security, Routing, Disjoint path, Real mobility data traces

1 Introduction

By design, OppNets typically incur a large delay, no assurance of end-to-end path, and intermittent connectivity between the sender and destination nodes. Furthermore, the existing single-copy and multi-copy techniques in OppNets lack multi-path routing that can greatly improve the network performance by effectively utilizing the available network resources. Indeed, in order to use multipath routing in OppNets for applications such as emergencies, crisis management, healthcare, to name a few, it is necessary that a secure communication be established among the nodes [1-2].

Multipath routing techniques have been used for network management objectives such as achieving Quality of Service (QoS), controlling the network congestion, improving the data transmission reliability, and designing fault-tolerant routing [3-8]. The challenges that are introduced by single copy and multi-copy OppNet routings such as constrained power supply, limited buffer space, and low-computational capabilities, have been addressed through multipath routing protocols. While various OppNet routing protocols [9-10] such as PRoPHet [11], Epidemic [12], HiBOp [13] work effectively in normal network scenario, they have to be substantially modified to work in hostile environments. In such environments where malicious nodes may be present, the aforementioned routing protocols raise serious security concerns.

Focusing on security and multipath challenges in OppNets, this paper proposes a secure routing technique (called D-MUST), which breaks the message into parts and relays these parts to the destination through four disjoint paths, each applying a soft-encryption technique to prevent message fabrication attacks. Soft encryption is applied to increase the network performance efficiency and to use resources. It should be noted that this technique does not make use of key transfers and key distribution centers.

The following sections discuss the different parts of the work. Section 2, presents related work. In Section 3, the proposed D-MUST protocol is described. Section 4, presents the analysis of results obtained from simulations. Finally, the last section presents the summation of the proposed work.

*Corresponding Author: Jagdeep Singh; E-mail: jagdeepknit@gmail.com
DOI: 10.3966/160792642019102006001

2 Related Work

To the best of our knowledge, there is no work in the literature on secure multipath routing for OppNets. Therefore, the work described in this paper is based on ad-hoc and sensor wireless networks.

In [14], Lou proposed a multipath routing protocol for wireless sensor network that improves the data transfer reliability. Their scheme is composed of two stages. First, the sink node broadcasts a route update message for root discovery purpose; and this initial flooding constructs a spanning tree structure. In the next phase, the multi-path extension flooding technique is utilized and alternate paths toward the sink are established; leading to improved packets delivery. However, the considered simple flooding technique does not result in routes interference. The limitation of this technique is that the physical proximity of the nodes and the concurrent data communication in the paths contribute in degrading the network performance.

In [15], Lou and Kwon proposed an N-to-1 multiple path routing and data communication security technique (called H-SPREAD) that can be used for increasing the path resilience against node failure. In their scheme, the sender node divides each data message into different shares and a secret sharing strategy is utilized for transmitting these shares toward the sink node using different paths. The limitation of this scheme is that it only improves the delivery rate and reliability in the network, but does not deal with the security of individual nodes.

In [16], Felemban et al. proposed a multipath-based packet delivery mechanism that relies on the SPEED protocol [17] and provides Quality of service (QoS) differentiation with regards to reliability. To guarantee a timeliness packet delivery, appropriate speed layers are assigned to data packets in such a way that the highest priority packets are processed before the lowest priority ones. When the source terminal wishes to transmit a packet to the receiver terminal, the so-called speed requirement of the message is calculated and the speed layer is chosen accordingly. Based on this, a routing decision is made in such a way as to satisfy the requirement of the data packet.

In [18], Huang and Fang investigated the delay and reliability constraints in QoS routing, and proposed a multi-constrained QoS multipath routing technique (called MCMP) for wireless sensor networks, which uses the multi-paths between the origin and end station nodes for QoS provisioning. In this scheme, based on the link information, the QoS is mapped into the link information vector on a route. The main disadvantage of this protocol is data redundancy.

In [19], Bagula and Mazandu introduced the revised version of the scheme proposed in \cite{Huang}, where the energy optimization problem is addressed by using a novel mechanism that selects only the paths with lower energy consumption (as opposed to random paths) for message transmission purpose.

In [20], Hurni and Braun discussed in his paper, an AOMDV-based energy-efficient multipath routing for wireless sensor networks, which can be used to achieve low-latency and energy-efficient communication by using a cross-layer information in wireless technology. In this scheme, a routing management mechanism is used to construct a hop count path toward the destination, and when doing so, the data from the MAC layer is used to eliminate the transmission latency. The main downfall of this work is the fact that it is mandatory for sensor nodes to be aware of the neighbor/intermediate nodes.

In [21], Narula et al. present a secure protocol for message transmission in MANET, which uses trust-based multipath and soft-encryption. The trust-based multipath is meant to ensure that nodes that are less trusted are assigned a lower number of encoded segments of the message (compared to nodes that are highly trusted). This strategy is used to limit the access to the minimum information needed by potential malicious nodes to defeat the encryption strategy. On the other hand, the soft-encryption is meant to avoid using a Key Distribution Center as well as a key transfer when performing the encryption.

In [22], Kandhoul and Dhurandher designed an asymmetric cryptography mechanism based on RSA for OppNets. In this work, cryptography is used to detect misbehaved nodes and to control the trust in an OppNet. The RSA algorithm is utilized to assure the integrity, confidentiality, non-reputability and authenticity of the messages. This approach protects the user from eavesdropping and other cryptographic attacks.

In [23], Sharma et al. introduced a secure routing by making predictions based on historical behavior of nodes. In the training phase, the forwarding time of each node is flooded in the environment scenario. In this test phase, only greyhole and blackhole nodes are detected when the mean forwarding time deviates from the absolute value. However, this mechanism cannot be used rest of the attacks such as denial-of-service, poisoning of messages etc.

2.1 Motivation

Unlike the above-discussed work, the proposed D-MUST routing protocol for OppNets makes use of four disjoint paths and a soft-encryption technique without key exchange to securely and opportunistically relay the messages from source to destination nodes. By simulations, its performance in terms of detecting blackhole and greyhole attacks is compared against that of the asymmetric RSA based Security protocol (RSASec) [22] and the History-Based Secure Routing Protocol (SHBPR) [23] and using the *HAGGLE INFOCOM 2006* real mobility data traces [24], demonstrating its superiority. The comparison of proposed D-MUST routing protocol with RSASec and

SHBPR is because of the following reasons: (1) RSASec and SHBPR are the most recent routing protocols and have already solve many routing related challenges. Comparison with these models would further improve the shortcomings. (2) RSASec and SHBPR favor hard encryption technique whereas D-MUST favors soft encryption where in less usage of resources like energy, encryption - decryption time etc. are consumed. (3) D-MUST follows disjoint multipath based secure routing, which is not followed by RSASec and SHBPR. (4) Lastly, the proposed D-MUST runs on real mobility traces where as SHBPR does not.

3 D-MUST Routing Protocol

The proposed D-MUST secure multipath routing protocol for OppNets operates in two phases. First, the message at the origin node is partitioned into four parts, each of which is encrypted using the XOR mechanism [21]. After securing the message parts using soft-encryption, each part is transmitted through disjoint paths to the destination, in such a way that the message-parts cannot be used to replicate the whole message. In the second phase, the message parts received at the destination are decrypted individually using again the XOR mechanism [4]. These decrypted message parts are then combined to obtain the required output if all the message parts are unaltered.

3.1 Assumptions

The following assumptions have been used in the design of the proposed D-MUST routing protocol:

(1) A_1: The sender node creates a message of $4n$ bits. Each n bits represent one part of the whole $4n$ message. The parts are represented as m_1, m_2, m_3 and m_4. These message parts are then forwarded on the basis of the unique part ID on each path. All the message parts are transmitted via disjoint routes. This design is assumed because it is easily implementable and require less computational resources.

(2) A_2: If a node, say n_1, has a part of the message and encounters another node, say n_2, which has the next part of that same message while transmitting the summary vectors, then n_2 will not be eligible for exchanging its summary vector with that of n_1, because such exchange would lead to one malicious node collecting more parts of the same message and easily decrypting it. In this case, the malicious node will be able to make changes in the message.

3.2 System Model

Assume that a network of N nodes exist in an OppNet. Suppose that a sender node requires to transmit a message to the end station node D.

If $u = u_1, u_2, u_3 \ldots\ldots u_n$ and $v = v_1, v_2, v_3 \ldots\ldots\ldots v_n$

Then

$$u \oplus v = u_1 \oplus v_1, u_2 \oplus v_2 \ldots\ldots\ldots\ldots\ldots u_n \oplus v_n. \quad \textbf{(1)}$$

3.3 Phase I: Message Encryption and Routing

The above-mentioned message parts m_1, m_2, m_3, and m_4 are encoded using the following equations:

$$m'_1 = m_1 \oplus m_2 \quad \textbf{(2)}$$

$$m'_2 = m_2 \oplus m'_1 \quad \textbf{(3)}$$

$$m'_3 = m_3 \oplus m'_2 \quad \textbf{(4)}$$

$$m'_4 = m_4 \oplus m'_3 \quad \textbf{(5)}$$

The new parts formed are m'_1, m'_2, m'_3 and m'_4 are then routed from source to destination using four disjoint paths. Each part m'_1, m'_2, m'_3 and m'_4 is set a unique ID. When a node is encountered in an OppNet, the following parameters are checked:

Delivery predictability. When the pair of nodes come within their communication range, they exchange their delivery predictability.

Summary vector. This vector consists of multiple properties such as message IDs, part IDs, hash values, sender IDs, and intermediate node IDs. When two nodes encounter each other, these vectors are also exchanged.

If the delivery predictability is high, the summary vectors are exchanged after confirming that no other message part already exists on that node. If any part of the message already exists on that node, no message will be exchanged. This process is repeated on all nodes in the paths established by the pair of the sender and destination nodes, hence creating disjoint paths. As a result, the parts of the message are routed to the destination node via these disjoint intermediate nodes using the aforementioned two phase procedure. The pseudo code of the proposed protocol is given in Algorithm 1. The various notations used in this work are explained in Table 1.

Algorithm 1. D-MUST Routing Protocol

1. Initially, the Source node creates a message M of 4n bits for transmitting to the Destination node.
2. Next, the Source node divided the message (M) into 4 equivalent parts, then each part is encrypted using XOR and assign a unique ID.
3. Compute for encryption
   $m'_1 = m_1 \oplus m_2$
   $m'_2 = m_2 \oplus m'_1$
   $m'_3 = m_3 \oplus m'_2$
   $m'_4 = m_4 \oplus m'_3$
4. When a new node $_j$ is encountered.

5. **If** ($node_j$ is not the destination) **then**
6. **If** (delivery pred. of nodej > $node_i$/$Source_{node}$) **then**
   exchange the summary vectors between $node_i$ /$Source_{node}$ and $node_j$.
   If (any part of the message exists at $node_j$) **then**
   Do not transfer the packet.
   EndIf
   Else
   Create a duplicate copy of the message part and transfer this copy to $node_j$, then update the summary vectors of both nodes.
   EndIf
7. **Else** ($node_j$ is the destination) **then**
   Transfer the message part to nodej and check all four parts of the message.
   If (All four parts have been received) **then**
   Compute for decryption and encapsulate the message *M* by using all parts after verification.
   $m_4 = m'_4 \oplus m'_3$
   $m_3 = m'_3 \oplus m'_2$
   $m_2 = m'_2 \oplus m'_1$
   $m_1 = m'_1 \oplus m_2$
   End If
   End If
8. Message delivered successfully at the Destination node.

Table 1. Notations

Notation	Description
$Source_{node}$	Source Node
$Destination_{node}$	Destination Node
M	Message of $4n$ bits
m_1	Part1 of the message
m_2	Part 2 of the message
m_3	Part 3 of the message
m_4	Part 4 of the message
m'_1	Encrypted Part 1 of the message
m'_2	Encrypted Part 2 of the message
m'_3	Encrypted Part 3 of the message
m'_4	Encrypted Part 4 of the message

3.4 Phase II: Message Decryption and Verification

The four encrypted message parts received at the destination node via the intermediate nodes are decrypted and verified in this phase. After this, each of the message parts is individually decrypted at the destination node using the following equations:

$$m_4 = m'_4 \oplus m'_3 \quad \textbf{(6)}$$

$$m_3 = m'_3 \oplus m'_2 \quad \textbf{(7)}$$

$$m_2 = m'_2 \oplus m'_1 \quad \textbf{(8)}$$

$$m_1 = m'_1 \oplus m_2 \quad \textbf{(9)}$$

After decryption, m_1, m_2, m_3, and m_4 message parts are retrieved. The hash value obtained is then used for verifying that all the message parts m_1, m_2, m_3, and m_4 are unaltered and un-fabricated. The hash calculation is performed using Equation (10). Finally, the original message is recovered from these message parts.

$$Hash(M) = m_1 << 5 \oplus m_2 << 5 \oplus m_3 << 5 \oplus m_4 \quad \textbf{(10)}$$

In an OppNet environment, as shown in Figure 1, the sender node *S* wishes to transmit the data to the end station node *D*. In this scenario, node *S* creates a message *M*, which is broken into four message parts m_1, m_2, m_3, and m_4 then encrypted using a XOR mechanism, yielding the message parts m'_1, m'_2, m'_3 and m'_4. These message parts are then forwarded on the basis of the unique part ID on each path. All the message parts are transmitted via disjoint routes. In Figure 1, we have shown only the route information for m'_1, which is *(S, 1, 8, 6, 7, 9, D)*. Other parts of the message follow a similar pattern as m'_1 to reach the destination node. Suppose, there are 20 nodes are present in the scenario. The considered route for all four parts m'_1, m'_2, m'_3 and m'_4 are *(S, 1, 8, 6, 7, 9, D), (S, 2, 5, 6, D), (S, 3, 13, 15, D)* and *(S, 4, 14, 9, 16, 18, D)* respectively. If any of the intermediate nodes is malicious, then these message parts may be fabricated by that node. Through simulations, it was found that the source *S* was able to transmit the message to the destination *D* successfully even though no complete route exists between them.

4 Simulation Analysis

The proposed D-MUST routing technique has been simulated and compared against that of two benchmark routing protocols: RSASec [22] and SHBPR [23], using the ONE simulator [25] and the *HAGGLE INFOCOM 2006* real mobility data traces. The network is modelled as a set of mobile nodes in which nodes may enter in the network or exit from the network at any time. The attack model implemented for these simulations is the message fabrication attack, where 10% of the nodes in each simulation behave maliciously. The simulation parameters are given in Table 2.

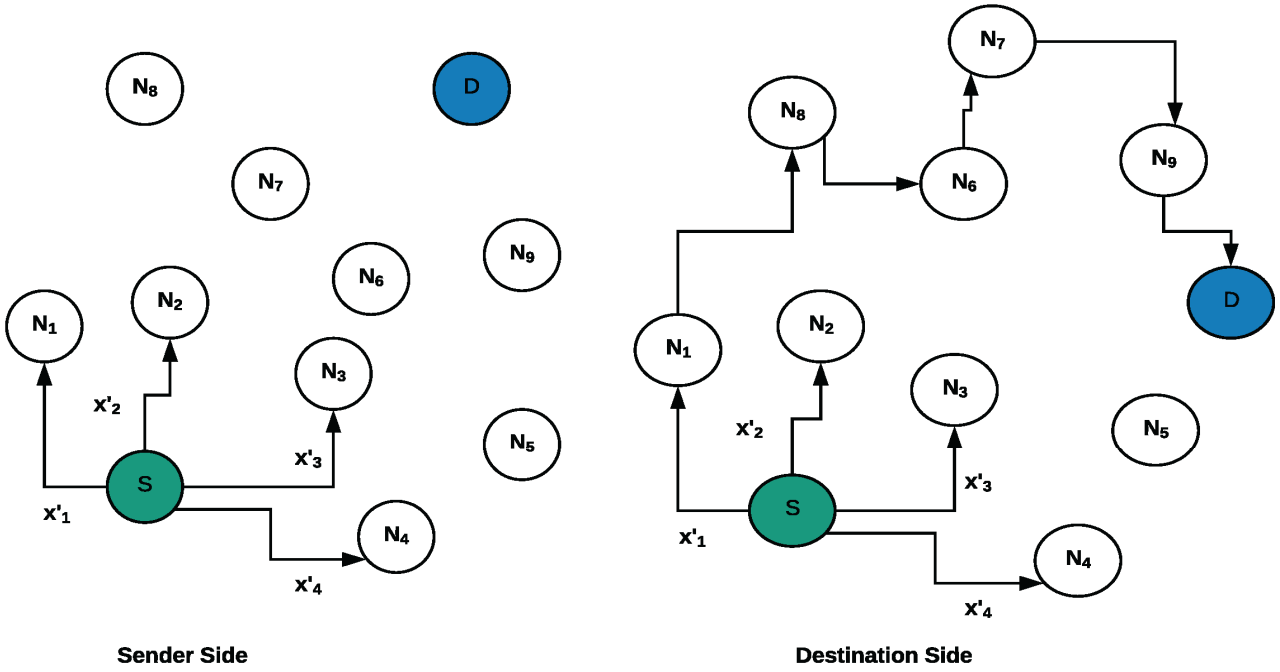

Figure 1. Illustrative example of D-MUST routing protocol

Table 2. Simulation parameters

Parameter	Value
Real Mobility Data Trace	Haggle Infocom 2006
Communication Interface	Bluetooth
Transmission range	10 m
Number of nodes	98
Number of contacts	170601
Simulation time	337418 seconds
Transmission speed	250 Kbps
Message size	500 Kb up to 1 Mb
Attack model	Message fabrication
Malicious node count	10%
Node movement model	Shortest path

The performance metrics for simulating the proposed D-MUST mechanism are messages dropped, delivery probability, hop count and average latency.

4.1 Simulation Results

First, Figure 2 is displayed between delivery probability and TTL (Time to Live) and observed that the delivery probability of D-MUST, RSASec, and SHBPR decreases as the TTL is increased. This is due to the fact that the time duration allotted to each message gets increased as the TTL increases, and when more messages gets stored in the node's buffer, the message delivery probability decreases. D-MUST yields the high delivery probability (0.35626) compared to that of RSASec (0.30262) and SHBPR (0.29864). Indeed, in terms of delivery probability, D-MUST is 15.05% better than RSASec and 16.17% better than SHBPR.

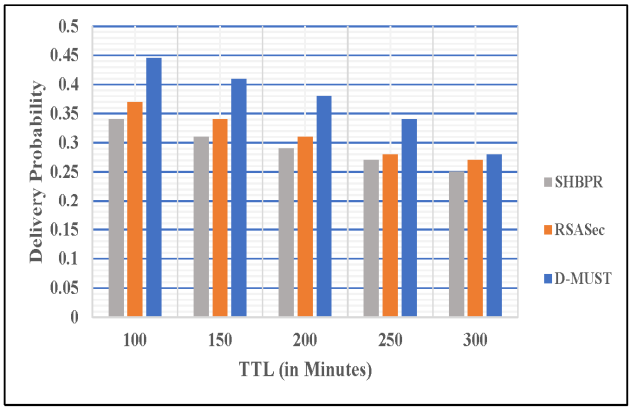

Figure 2. Delivery probability vs. TTL

Second, flow of hop count is pictured in Figure 3 as TTL varies. It is observed that D-MUST takes a lesser number of hops (compared to RSASec and SHBPR) to communicate the message.

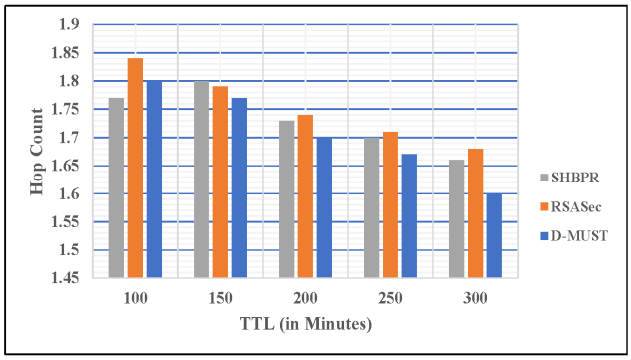

Figure 3. Hop count vs. TTL

Third, Figure 4 shows the relation between the number of messages dropped and TTL. It is analyzed that D-MUST yields the lowest number of messages dropped.

This is attributed to the criteria used in the design of D-MUST for selecting the best selector/relay of the message, and this contributes in minimizing the number of message dropped. In fact, in respect of number of messages dribbled, the performance of D-MUST is 5.81% better than that of RSASec and 6.85% better than that of SHBPR.

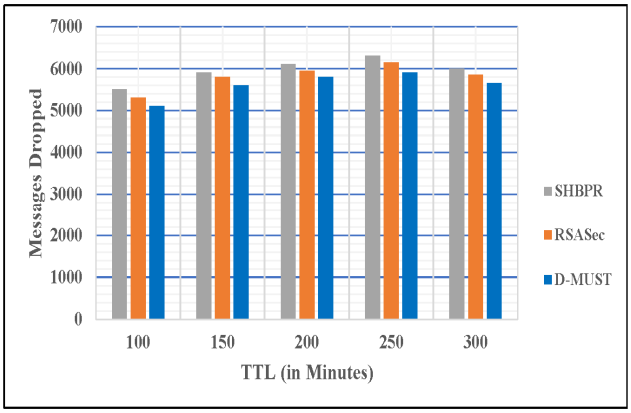

Figure 4. Message dropped vs. TTL

Fourth, the TTL is varied and the impact of this variation on the latency is investigated. The results are captured in Figure 5. It is observed that when the TTL is increased, the average latency also increases. This is due to the fact that a substantial of TTL value also increases the stay of the message in the node's buffer. It is also observed that D-MUST yields the lowest latency compared to that generated by RSASec and SHBPR.

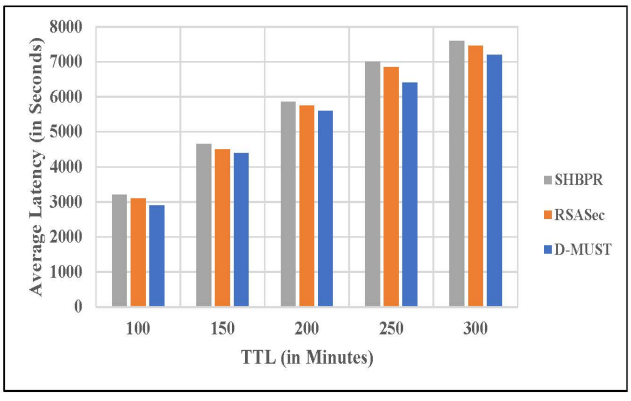

Figure 5. Average latency vs. TTL

In fact, in terms of latency, the performance of DMUST is 2.16% better than that of RSASec, and 3.95% better than that of SHBPR.

Figure 5 shows the dependence of the average latency with the TTL for all the scenarios. From the graph, it has been monitored that with the increase in TTL the average latency also increases. This occurs due to substantial TTL value increases the stay of the message in the node's buffer. The mean average latency value of D-MUST is the lowest among all the scenario/techniques that are 5375.2161 seconds. In context to this the performance of D-MUST is 2.16% better than RSASec, and 3.95% better than SHBPR respectively.

Fifth, the buffer capacity is varied and the effect of this change on the delivery probability is investigated. The performance of the protocols is captured in Figure 6. It is found that with increasing buffer capacity, the delivery probability is also increased. This is due to the buffer capacity of a node get large, the more number of messages stored in that buffer gets increased, leading to more messages getting delivered to the receiver node. In terms of delivery probability, the performance of D-MUST is 10.91% better than that of SHBPR and 6.57% better than that of RSASec.

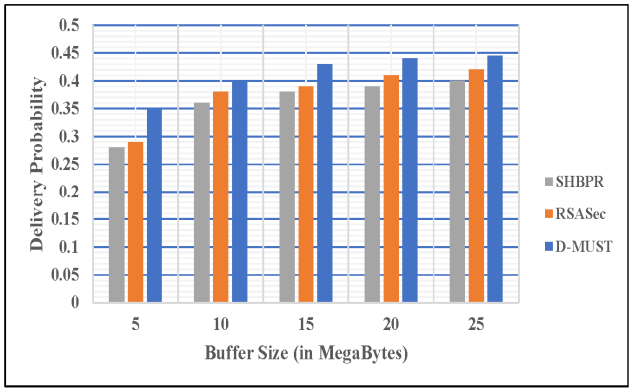

Figure 6. Delivery probability vs. buffer size

Sixth, the buffer capacity is varied and the effect of this change on the number of hops (resp. messages dropped) is investigated. The performance of the protocols is captured in Figure 7 (resp. Figure 8). It is observed that when the buffer size is increased, the hop count (resp. messages dropped) also increases. The average hop count value is 1.60266 for DMUST, 1.69456 for SHBPR and 1.64692 for RSASec when the buffer size varies.

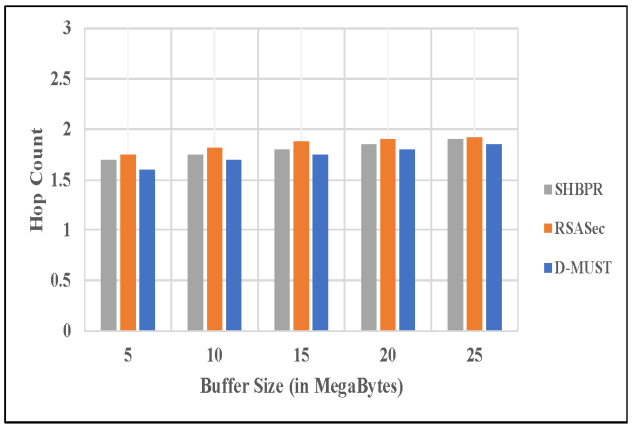

Figure 7. Hop count vs. buffer size

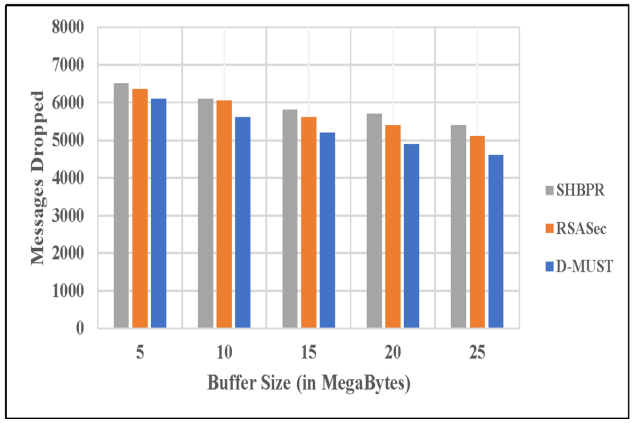

Figure 8. Message dropped vs. buffer size

Seventh, the buffer capacity is varied and the effect of this change on the average latency is investigated. The performance of the protocols is captured in Figure 9.

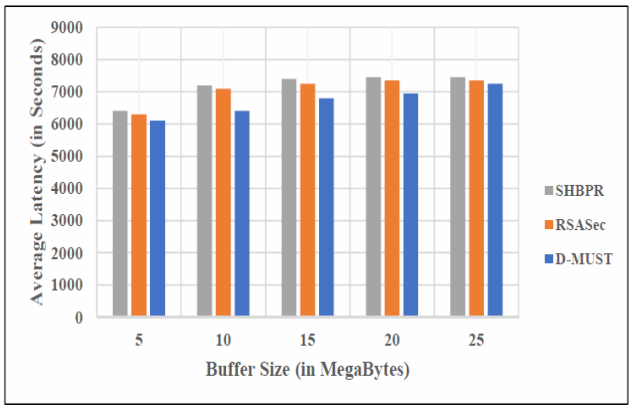

Figure 9. Average latency vs. buffer size

As expected, it is observed that D-MUST yields the lowest latency compared to that generated by RSASec and SHBPR. This is also attributed to the criteria used in the design of D-MUST for selecting the best forwarder of the message. It is also observed that as the buffer size increases, the average latency also increases. The average latency is 6693.88568 seconds for D-MUST, 7153.38936 seconds for RSASec and 7276.38492 seconds for SHBPR.

Eighth, the interval between the messages is varied and the effect of this variation on the hop count, average latency, number of messages dropped, and delivery probability are investigated. The performance of the protocols is captured in Figuret 10 to Figure 13. In Figure 10, it is observed that the probability of delivering the packet/message decreases, the interval between messages increases. This situation crop up owing to the few number of message creation in the network when the interval of the message increases, which in turns decreases the messages drop rate. In terms of delivery probability, the performance of D-MUST is 12.72% superior than RSASec and 13.35% superior than SHBPR.

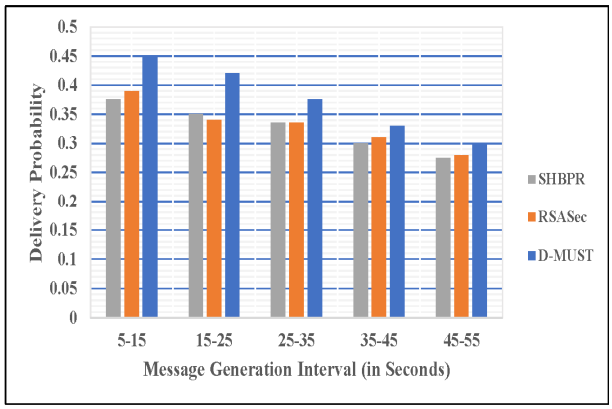

Figure 10. Delivery probability vs. message generation interval

In Figure 11, it is found that when the message generation interval is varied, the hop count is increased. The average hop count value is 1.50886 for D-MUST, 1.48606 for RSASec, and 1.52814 for SHBPR. In Figure 12, it is observed that when the message generation interval is varied in the network, there is a decrease in the number of messages dropped. Furthermore, the performance of D-MUST is 9.69% superior than RSASec and 10.63% superior than SHBPR.

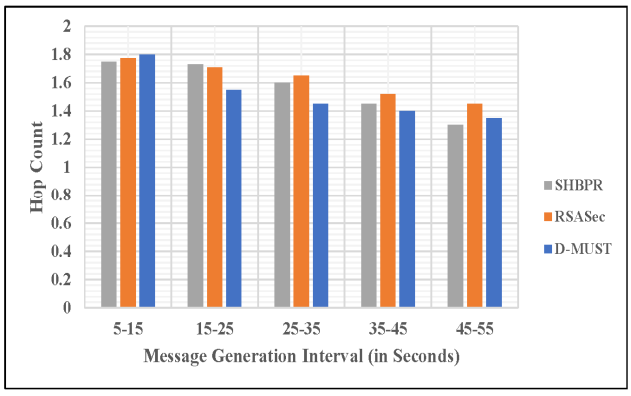

Figure 11. Hop count vs. message generation interval

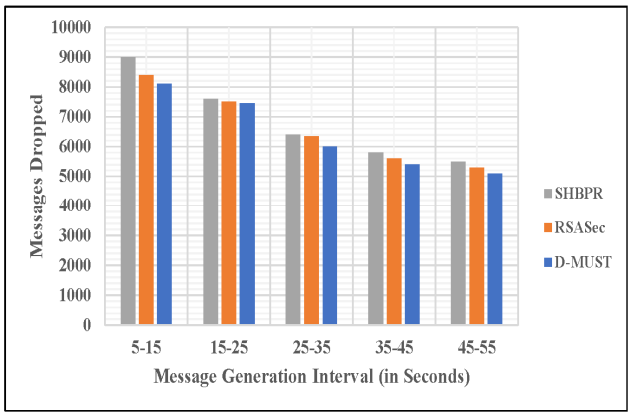

Figure 12. Message dropped vs. message generation interval

In Figure 13, shows that the average latency decreases while the message generation interval is varying, Also, D-MUST yields the lowest average latency among all schemes. Finally, in terms of latency, the performance of D-MUST is 9.89% superior than RSASec and 11.08% superior than SHBPR.

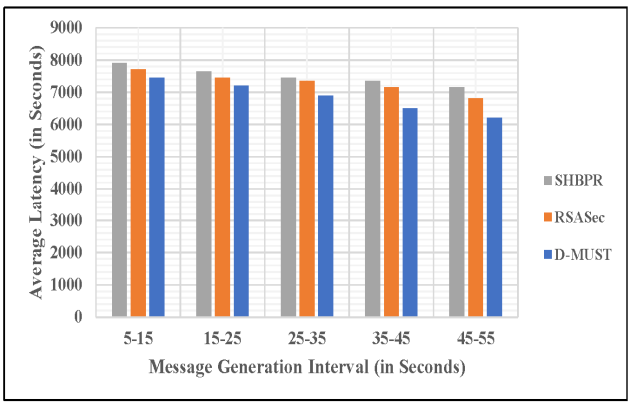

Figure 13. Average latency vs. message generation interval

Ninth, Figure 14 shows very interesting analysis. It shows that their whenever there is an increase in the TTL the buffer time also rises, which interprets that the nodes can keep the messages in their buffer for quite a long duration or might until and unless they are not delivered or its validity doesn't expire. The following statistics show the average buffer time for the different objectives when the TTL varies in the network. For (RSASec = 5605.73976 seconds), for (SHBPR= 5593.68638 seconds), and for (D-MUST = 5293.68638 seconds). The standard deviation is also evaluated in order to prove the resultsmore mathematically. For SHBPR, RSASec, and for D-MUST is 1920.805563, 1954.449832, and 1925.106335 respectively.

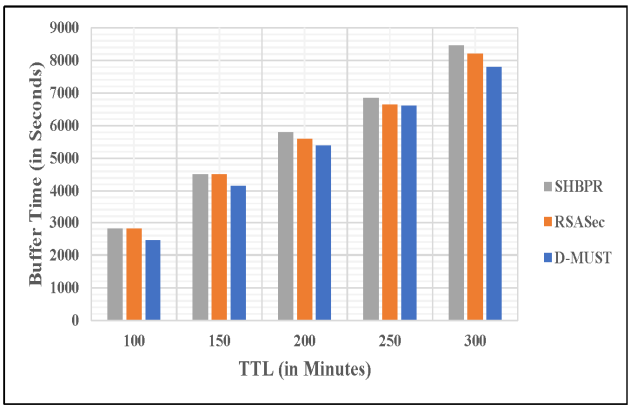

Figure 14. Buffer time vs. TTL

Tenth, as in Figure 15 the buffer time is decreasing as there is an increase in the message generation interval. This happens because the frequency of generating the message in the network is reduced therefore less number of messages will be stored in the buffer as and when the new message will be available it will be communicated fast as compared to other factors (fewer resource consumption). The message won't have to wait for a long time to be placed at least in the node's buffer. The obtained average buffer time is 8949.89976 seconds for RSASec, 9589.9976 seconds for SHBPR, and 9922.05 seconds seconds for D-MUST. Also, the standard deviation is 687.7719391 for RSASec, 988.0837654 for SHBPR, and 1277.814052 for D-MUST. These results show that D-MUST outperforms RSASec and SHBPR.

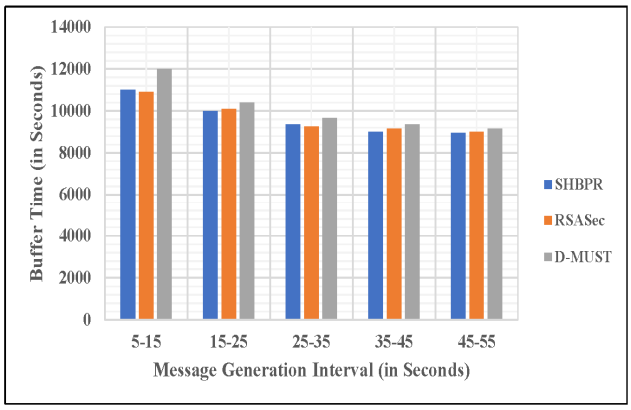

Figure 15. Buffer time vs. message generation interval

5 Conclusion

In this work, the author presented a novel secure multipath routing protocol for OppNets (called D-MUST), which relies on multipath and self-encryption features. Simulation results have shown that D-MUST outperforms SHBPR and RSASec, chosen as benchmark routing protocols for OppNets, in terms of average latency and delivery probability. In addition, from a practical perspective, D-MUST does not require high resources, high computation, or any form of key exchange. Further, the authors try to enhance the performance of DMUST on other real mobility traces such as the ones provided in [26-28] as future work.

Acknowledgments

This work is partially supported by a grant from the National Science and Engineering Research Council of Canada (NSERC) held by the third author, REF RGPIN/2017-04423; and by National Funding from the FCT– Fundação para a Ciência e a Tecnologia through the UID EEA/500008/2013 Project; and by Brazilian National Council for Research and Development (CNPq) via Grant No. 309335/2017-5, held by the 4th author.

References

[1] S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, LA-MHR: Learning Automata Based Multilevel Heterogeneous Routing

for Opportunistic Shared Spectrum Access to Enhance Lifetime of WSN, *IEEE Systems Journal*, Vol. 13, No. 1, pp. 313-323, March, 2019.

[2] S. K. Dhurandher, A. Kumar, M. S. Obaidat, Cryptography-based Misbehavior Detection and Trust Control Mechanism for Opportunistic Network Systems, *IEEE Systems Journal*, Vol. 12, No. 4, pp. 3191-3202, December, 2018.

[3] A. Kumar, S. K. Dhurandher, I. Woungang, M. S. Obaidat, S. Gupta, J. J. P. C. Rodrigues, An Altruism-based Trust-Dependent Message Forwarding Protocol for Opportunistic Networks, *International Journal of Communication Systems*, Vol. 30, No. 10, e3232, July, 2017.

[4] S. K. Dhurandher, V. Mehra, Multi-Path And Message Trust-Based Secure Routing in Ad Hoc Networks, *IEEE 2009 International Conference on Advances in Computing, Control, & Telecommunication Technologies* (ACT'09), Trivandrum, Kerala, India, 2009, pp. 189-194.

[5] J. Jin, S. Ahn, A Multipath Routing Protocol Based on Bloom Filter for Multihop Wireless Networks, *Mobile Information Systems*, Vol. 2016, Article ID 8151403, January, 2016.

[6] S. Kim, H. Cho, T. Yang, C. Kim, S.-H. Kim, Low-Cost Multipath Routing Protocol by Adapting Opportunistic Routing in Wireless Sensor Networks, *2017 IEEE Wireless Communications and Networking Conference (WCNC 2017)*, San Francisco, CA, USA, 2017, pp. 1-6.

[7] H. Lenando, M. Alrfaay, EpSoc: Social-Based Epidemic-Based Routing Protocol in Opportunistic Mobile Social Network, *Mobile Information Systems*, Vol. 2018, Article ID 6462826, April, 2018.

[8] D. Adami, C. Callegari, S. Giordano, M. Pagano, Single-Path And Multi-Path Label Switched Path Allocation Algorithms with Quality-Of-Service Constraints: Performance Analysis and Implementation in NS2, *IET Communications*, Vol. 6, No. 4, pp. 398-407, March, 2012.

[9] Q.-S. Cai, Y.-Q. Bai, G.-J. Han, C.-h. Pak, H. Zhao, An Energy-Saving Node Communicability Computation Scheme in Opportunistic Mobile Social Networks Using Cloud Assistance, *Journal of Internet Technology*, Vol. 17, No. 5, pp. 929-938, September, 2016.

[10] F. Wang, Z. Wang, Z. Yang, S. Chen, Contact Duration Aware Cache Refreshing for Mobile Opportunistic Networks, *IET Networks*, Vol. 5, No. 4, pp. 93-103, July, 2016.

[11] A. Lindgren, A. Doria, O. Schelen, Probabilistic Routing in Intermittently Connected Networks, *International Workshop on Service Assurance with Partial and Intermittent Resources*, Fortaleza, Brazil, 2004, pp. 239-254.

[12] A. Vahdat, D. Becker, *Epidemic Routing for Partially Connected Ad Hoc Networks*, Technical Report CS-200006, April, 2000.

[13] C. Boldrini, M. Conti, J. Jacopini, A. Passarella, Hibop: A History Based Routing Protocol for Opportunistic Networks, *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2007)*, Espoo, Finland, 2007, pp. 1-12.

[14] W. Lou, An efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks, *IEEE International Conference on Mobile Ad hoc and Sensor Systems Conference*, Washington, DC, USA 2005, pp. 1-8.

[15] W. Lou, Y. Kwon, H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks, *IEEE Transactions on Vehicular Technology*, Vol. 55, No. 4, pp. 1320-1330, July, 2006.

[16] E. Felemban, C.-G. Lee, E. Ekici, MMSPEED: Multipath Multi-SPEED Protocol for Qos Guarantee of Reliability and Timeliness in Wireless Sensor Networks, *IEEE Transactions on Mobile Computing*, Vol. 5, No. 6, pp. 738-754, June, 2006.

[17] T. He, J. A. Stankovic, C. Lu, T. F. Abdelzaher, SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks, *23rd International Conference on Distributed Computing Systems (ICDCS 2003)*, Providence, Rhode Island, USA, 2003, pp. 46-55.

[18] X. Huang, Y. Fang, Multiconstrained QoS Multipath Routing in Wireless Sensor Networks, *Wireless Networks*, Vol. 14, No. 4, pp. 465-478, August, 2008.

[19] A. B. Bagula, K. G. Mazandu, Energy Constrained Multipath Routing in Wireless Sensor Networks, *Proc. of the International Conference on Ubiquitous Intelligence and Computing*, Oslo, Norway, 2008, pp. 453-467.

[20] P. Hurni, T. Braun, Energy-Efficient Multi-Path Routing in Wireless Sensor Networks, *Proc. of the 7th International Conference on Ad-Hoc, Mobile and Wireless Networks (ADHOC-NOW)*, Sophia-Antipolis, France, 2008, pp. 72-85.

[21] P. Narula, S. K. Dhurandher, S. Misra, I. Woungang, Security in Mobile Ad-Hoc Networks Using Soft Encryption and Trust-Based Multi-Path Routing, *Computer Communications*, Vol. 31, No. 4, pp. 760-769, March, 2008.

[22] N. Kandhoul, S. K. Dhurandher, An Asymmetric RSA-based Security Approach for Opportunistic IoT, *Proc. of International Conference on Wireless Intelligent and Distributed Environment for Communication (WIDECOM 2018)*, Toronto, ON, Canada, 2018, pp. 1-14.

[23] D. K. Sharma, S. K. Dhurandher, I. Woungang, J. Arora, H. Gupta, History-based Secure Routing Protocol to Detect Blackhole and Greyhole Attacks in Opportunistic Networks, *Recent Advances in Communications and Networking Technology*, Vol. 5, No. 2, pp. 73-89, 2016.

[24] CRAWDAD Dataset Cambridge HAGGLE, https://crawdad.org/uoi/haggle/20160828/one (Last accessed March 10, 2019)

[25] A. Keranen, J. Ott, T. Karkkainen, The ONE Simulator for DTN Protocol Evaluation, *Proc. of the 2nd International Conference on Simulation Tools and Techniques (SIMUTools' 09)*, Rome, Italy, 2009, pp. 1-9.

[26] I. Rhee, M. Shin, S. Hong, K. Lee, S. J. Kim, S. Chong, On the Levy-walk Nature of Human Mobility, *IEEE/ACM Transactions on Networking*, Vol. 19, No. 3, pp. 630-643, June, 2011.

[27] K. Massri, A. Vitaletti, A. Vernata, I. Chatzigiannakis, Routing Protocols for Delay Tolerant Networks: A Reference Architecture and a Thorough Quantitative Evaluation, *Journal of Sensor and Actuator Networks*, Vol. 5, No. 2, p. 6, June, 2016.

[28] J. A. Dias, J. N. Isento, V. N. G. J. Soares, F. Farahmand, J. J.

P. C. Rodrigues, Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks, *Proc. of the IEEE GLOBECOM Workshops (GC Wkshps)*, Houston, TX, USA, 2011, pp. 51-55.

Biographies

Sanjay K. Dhurandher received the M.Tech. and Ph.D. degrees in Computer Science from the Jawaharlal Nehru University, New Delhi, India. He is currently working as a Professor in the Department of Information Technology, Netaji Subhas University of Technology (*Formelry NSIT*), New Delhi. From 1995 to 2000, he worked as a Scientist/Engineer at the Institute for Plasma Research, which is under the Department of Atomic Energy, India. His current research interests include wireless ad hoc networks, sensor networks, computer networks, opportunistic networks, network security, and underwater sensor networks. Dr. Dhurandher currently serves as the *Associate Editor* of Wiley's International Journal of Communication Systems. He is also a Senior Member of IEEE.

Jagdeep Singh is pursuing Ph.D. from Division of Information Technology, Netaji Subhas Institute of Technology, University of Delhi. He received his M.Tech in Computer Science and Engineering from Kamla Nehru Institute of Technology, Sultanpur, India. His areas of expertise include opportunistic networks, cloud computing, fog computing etc. He has presented papers in international conferences and published research work in various international journals.

Isaac Woungang received his M.Sc. & Ph.D. degrees, all in Mathematics, from University of Aix-Marseille II, and University of South, Toulon and Var, France, in 1990 and 1994 respectively. Since 2002, he has been with Ryerson University, where he is now a Professor of Computer Science and Director of the Distributed Applications and Broadband (DABNEL) Lab. His current research interestsinclude radio resource management, computer security, heterogeneous networks, computationalintelligence and machine learning applications, performance modelling, analysis and optimization.

Joel J. P. C. Rodrigues [S'01, M'06, SM'06] is a professor at the Federal University of Piauí, Brazil; and senior researcher at the Instituto de Telecomunicações, Portugal. Prof. Rodrigues is the leader of the Internet of Thingsresearchgroup (CNPq), Director for Conference Development - IEEE ComSoc Board of Governors, IEEE Distinguished Lecturer, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the Past-Chair of the IEEE ComSoc Technical Committee on eHealth, the Past-chair of the IEEE ComSoc Technical Committee on Communications Software, Steering Committee member of the IEEE Life Sciences Technical Community and Publicationsco-Chair. Heis the editor-in-chief of the International Journal on E-Health and Medical Communications and editorial board member of several high-reputed journals. Hehasauthoredor coauthored over 750 papers in refereed international journals and conferences, 3 books, 2 patents, and 1 ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. Prof. Rodrigues is a licensed professional engineer (as senior member), member of the Internet Society, and a senior member ACM and IEEE.