Encounter Record Trust-based Scheme against Flooding Attack in Delay Tolerant Networks

Pooja R. Makawana, Rutvij H. Jhaveri

***Abstract*— Delay/Disruption Tolerant Network (DTN) is a rising communication criterion distinguished by intermittent connectivity. Routing algorithms in DTN are developed with the simple hypothesis that all the participating nodes collaborate with each other in storing and forwarding packets. Due to lake of centralized authority, it is difficult to protect the network against non-cooperative nodes. There may be some malicious nodes which may disrupt the forwarding strategy and insert excessive spurious traffic in order to degrade the performance of the network. This kind of misbehavior is known as *Flooding attack*.**

This paper addresses this issue by using encounter record based scheme along with the trust based scheme to prevent network against Flooding attack. Encounter record table is used to check the encounter history of the receiver node and a trust metric is used to evaluate legitimacy of the received messages. Simulation outcomes show that our proposed scheme reduces the spurious traffic into the network which gives increased results for delivery probability and reduced overhead ratio.

Index Terms— **Delay tolerant network, Flooding attack, Forwarding strategy, Routing security, Trust-based routing.**

I. Introduction

DELAY/DISRUPTION TOLERANT NETWORK (DTN) is established to contract with challenged environments characterized by frequent network partitions, intermittent connectivity and variable delay DTN has gained enormous popularity in critical applications such as post-disaster scenarios[3][4], deep-space communication[5][6][7][8], interplanetary applications, terrestrial scenarios and many more[9]. DTN is intermittently connected network means that the complete path from source to destination may not exist. Nodes may be intermittently connected as shown in Fig.1. [1].

DTN is having exclusive features like multiple nodes, self-organization and no central authority [2]. It uses "Store-Carry-Forward" strategy regardless of availability of an end to end path between source nodes to destination node. Each intermediate node will store the packet into its buffer space and carries the message with itself until it encounters the next node and forward the message to the encountered node based on some predefined metric or forwarding strategy [10]. So, the packets are opportunistically routed toward the destination.

Routing protocols does the key role for efficiently forwarding the data packets in DTN. Various routing protocols are proposed to find a potential forwarder to the destination based on probabilistic or social conduct of encountered nodes. Although DTN can be threatened because of forwarding misbehavior.

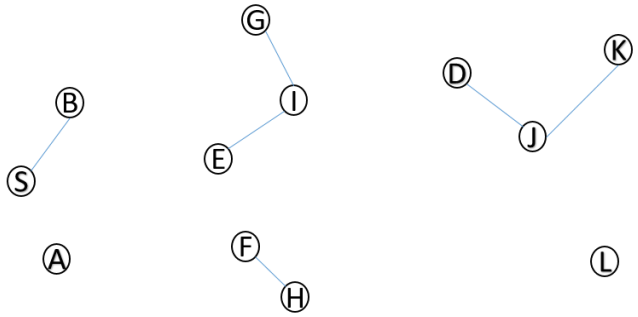

Fig. 1. Intermittently connected network.

Security of DTN has been an imperative area of research due to the upswing in popularity of DTN. There are numerous strategies proposed to against security threats in DTN. The strategies proposed to cope with misbehaving nodes can be classified into three categories, *reactive approach* in which first the malicious node is detected and then prohibitive action is taken against it [11][12], *proactive approach* such as credit based incentive techniques where credits are awarded to the cooperative nodes[13], [14] and *user-interest based approach* groups are created based on user–concern and social ties.[1]. DTN is threatened from various attacks like black hole attack, grey hole attack and so on[2]. One of the most effective threats in DTN is flooding attack. In flooding attack, a malicious node builds a path toward the other nodes and sends the spurious traffic to encountered nodes which propagates all over the network and causes the network to be exhausted. Malicious nodes may insert number of replicas of some genuine message to place the flooding attack into the network. This spurious messages will be further forwarded by the genuine nodes unaware of the forged messages. This may cause the waste of bandwidth and drained batteries which results reduced network performance.

There are three types of flooding attacks. *Message flooding* in which excessive spurious messages are injected into the network. *Replica flooding* in which replicas of genuine messages are inserted into the network, *Spoof flooding* in which the malicious node pretends to be a different entity[12].

P. R. Makawana is with the Information Technology Department, Shri S'ad Vidya Mandal Institute of Technology, Bharuch, INDIA.

R. H. Jhaveri is with the Computer Engineering/Information Technology Department, Shri S'ad Vidya Mandal Institute of Technology, Bharuch, INDIA.

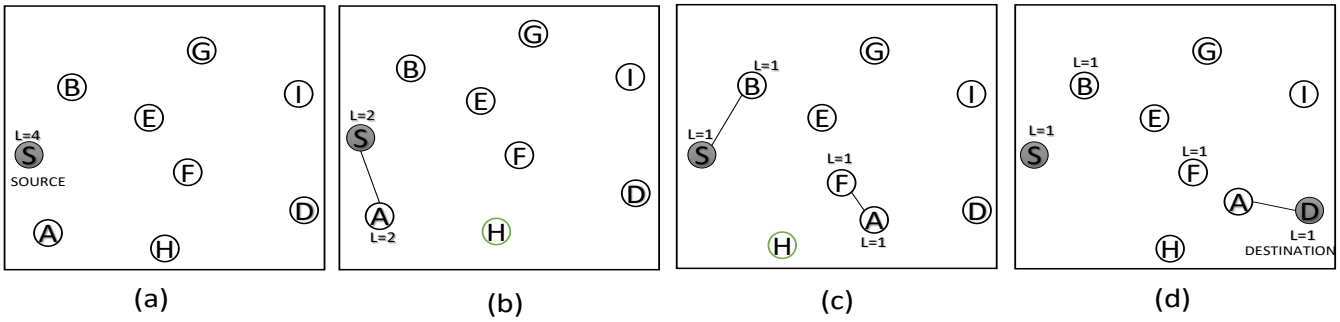

Fig. 2. Binary Spray and Wait in DTN **a**, **b**, **c** Spray Phase **d** Wait Phase.

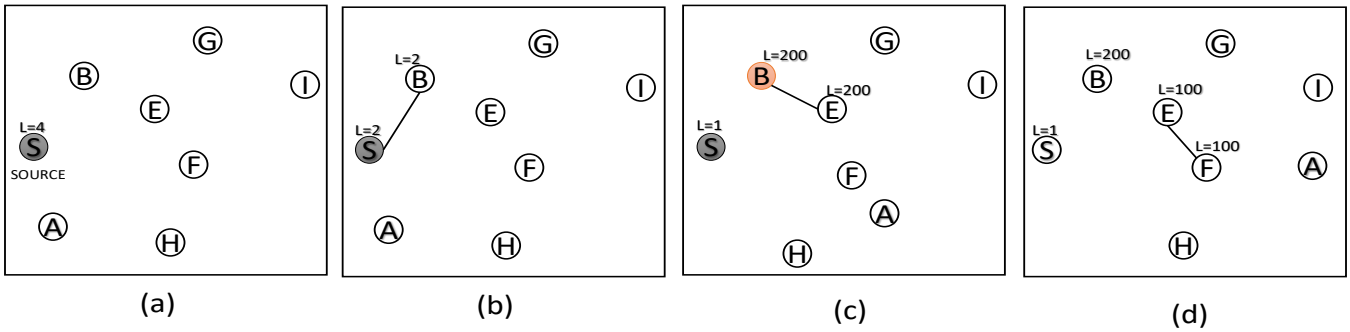

Fig. 3. Flooding Attack in Spray Phase of binary Spray and Wait in DTN.

Forwarding behavior directly depend on the routing protocol. Numerous routing protocols have been proposed in DTN like 'Epidemic', 'Spray and Wait' and 'PRoPHET' each having a different forwarding strategy. Here we focus on the routing protocol named 'Spray and Wait' protocol.

The rest of the paper is organized as follows: Section II contains related work which motivates our work, Section III presents overview of flooding attack and basic ideas behind our scheme, Section IV presents proposed scheme, Section V presents simulation results and analysis and Section VI presents conclusion.

II. Related work

In past few years, various reactive strategies are proposed to combat flooding attacks in DTN. Godwin et al.[15] proposed a strategy based on DTN cookie. Network is divided into multiple groups and one group head is allocated to all the groups. Checking the authenticity of forge of packet is responsibility of the group head and according to network threat level the DTN cookie is chosen. Even though, it is possible to measure the network threat level, they have not considered replica flooding which can impact heavily on network overhead. Qinghua et al.[16] proposed rate limiter technique along with the claim-carry-check mechanism. Each node claims for the sent messages of itself. There is a pre-defined set rate limit to the sent messages of all the nodes. They all will claim for their sent messages and transmit the claim with each packet. All the newly generated packets will compute a signature to authenticate the packet. This scheme is quiet efficient in detecting the malicious nodes but the communication and computation cost is the matter of consideration. Xixiang et al.[7] proposed a non-interactive key exchange protocol. Node generates a long term public key at the time of the encounter with the other node and they will exchange the public keys which will protect against unauthorized access and prevent the network from DOS attack. They have not considered flooding based DOS attacks. Hang et al.[2] proposed an evolutionary game theory to defend against various kind of attack. They use game theory based approach to analyze and simplify the routing behavior of the nodes in the network. Based on that the misbehaving nodes are identified. Chauah et.al[17] proposed a ferry based detection scheme which uses trusted ferry nodes to test the authenticity of the other nodes. It is particularly used for prophet routing algorithm. Improved version of FBDIM is proposed by Ren et al.[18] Is MUTON which uses transitivity property and it also uses ferries as trusted nodes. Although it is a good mechanism for detection but its overhead ratio is very large. Sujoy et al.[1] proposed a connected trusted nodes and connected trusted node with malicious list for detection and removal of malicious nodes causing denial of service attack. But they have not considered the replica flooding attack in binary tree based spray and wait algorithm. Pham et al.[12] proposed a strategy for detection of flooding attack by using the encounter record table. They check the list of sent messages in the encounter record table which should not exceed the pre-defined threshold for sent messages. The node exceeding the threshold is detected as an attacker node. The overhead and delivery probability is not considered here and they have assumed that occurrence of false positives is nil. Natarajan et al. proposed an approach in defense of overusing the buffer space. Doina et al.[19] proposed an evolutionary algorithm based strategy coupled with the network simulator. This algorithm is specifically designed for the problems which are decomposable into multiple small problems. They have addressed flooding attack and DOS based on flooding. They have not considered replica flooding attack. Feng et al.[20] proposed a queuing mechanism using ferry nodes. They differentiate the malicious nodes and detect flooding attack using queuing policy along with PRoPHET routing algorithm. They do not address the replica flooding attack.

Motivation existing works shows various reactive strategies like stream check and encounter record based techniques of DTN-cookies and many more. Each having different drawbacks in terms of throughput and overhead. In some case false positives are not discussed or the replica flooding is not considered. Drawbacks of such existing scheme motivated us to do the proposed work

Objective of this paper is to devise a Routing algorithm that is useful in detection and prohibition of the flooding attack and affected malicious nodes. To protect the resources from being misused we reduce the amount of replicated messages so that the original genuine messages can get fair chance to propagate towards the destination

III. Overview

A. Flooding Attack and Binary Spray and Wait Routing Protocol

Flooding attack and Binary Spray and Wait routing protocol: Binary Spray and wait protocol is updated version of Spray and Wait protocol. It consists of the following two phases.

Spray Phase: In Binary spray phase the source node will generate L number of copies and forwards L/2 number of copies to the first encountered relay node (i.e node A). Now A will have m number of copies. Any relay node having m>1 number of copies will forward m/2 number of copies to next encountered node.[21]

Wait Phase: If the destination node is not encountered in the spray phase then each relay node will go for direct delivery to the destined node. They will store the message until the destination is found. The nodes may also discard the messages because of limited buffer space or limited life span of the message[21]

As shown in Fig.2 node S have generated 4 number of copies out of which 2 will be forwarded to next encountered node A. Now S and A both will contain 2 copies of the message. A will forward one copy to the next encountered node that is F. S will forward one copy to B. Finally, all the relay nodes will contain one copy of the message and they will go for direct delivery until the destination is encountered.

As shown in Fig.3 any node can be a malicious node and it may insert spurious traffic into the network. Here node B is attacker node which is inserting excessive number of spurious replica into the network. Other node who are unaware of malicious ness of the attacker node will propagate the spurious messages all over the network. So the bandwidth and the buffer space of the node will be wasted for the spurious message and all over performance is degraded in terms of overhead and delivery probability of genuine messages.

Simulation results shows the impact of replica flood attack on various parameters while using Spray and wait routing algorithm. It is observed that while increasing number of attackers in the network it makes the negative impact on network performance. We have varied six to twelve number of attackers. No of dropped messages are increased while increasing number of attackers. Latency is also increased because of increase in spurious messages.as a result of this overall network overhead is increased.

B. Adversary model

There may be various kind of attacker in the network. In replica flooding, attacker inject multiple spurious replicas of a message into the network. An attacker can be a sender node or a source node which is inserting Replicas. Accepting Message from such node is not a good choice. Secondly, an attacker may be a receiving node which accepts messages from encountered node and replicate that genuine messages and flood into the network.

C. Calculating threshold value L

As discussed above in spray and wait routing protocol during spray phase utmost L replicas are sprayed. So, we can say that a node is not allowed to send more than L replicas of a single message. We take this L value as a threshold for no. of sent replicas.

Upper bound for an expected delay for spray and wait protocol is ED_{opt} [21]. An equation to choose minimum value of L to achieve expected delay aED_{opt} (a times the optimal delay where a>1) is independent of transmission range and size of the network. It only depend on the number of nodes N. Value of L can be calculated using the above Eq. (1) is derived from the theory proposed by the cauligi et al.[21].

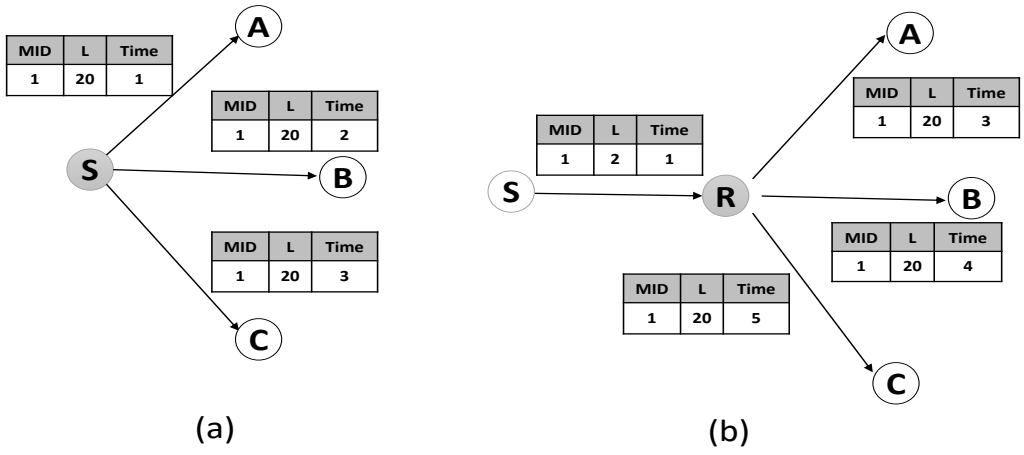

Fig. 4. Replica flooding (a) Sender as an attacker (b) Relay node as an attacker

$$a\left(\frac{H_{N-1}}{N-1}\right) = H_{N-1} - H_{N-L} + \frac{N-L}{N-1}\frac{1}{L} \quad (1)$$

Where H_n is the n^{th} Harmonic Number i.e. $H_n = \sum_{i=1}^{n} \frac{1}{i}$

D. Calculating Trust Value.

Here we consider two type of trust (1) Direct trust and (2) Indirect trust. Direct trust is calculated when two nodes are encountered. When a node is sending valid number of replica its trust value is higher. Indirect trust is calculated transitively by considering other nodes recommendations of their trust metric. For that we consider number of messages sent by a node. A node which encounters often and sends more than allowed number of replica, its trust metric is decremented by α value. Initial trust at the starting of simulation is taken as a static value say β. We can say that trust metric keeps track of the nodes whose forwarding behavior is more accurate and trustworthiness of a node. Eq. (2) demonstrate that how to calculate trust transitively.

$$TV_A C = TV_A C \cdot old + RT_B \cdot C \pm \alpha \quad (1)$$

Where $TV_A C$ is trust value of node C into A's table.

Here α is considered as a reward or punishment in case of direct trust calculation.

IV. Proposed Scheme

In this section we propose a trust based approach along with the encounter record based scheme. We consider two scenarios in first scenario sender node is an attacker. This sender can be a source itself. Second is the relay node is an attacker. For evaluation of a node we consider no. of sent messages in node's encounter record table and its trust value.

A. Detection of Relay node as an attacker

As shown in Fig.4 (b) attacker relay node will accept genuine messages from the sender or other relay node unaware of the attacker. Malicious relay will replicate that messages and flood them into the network. This flooded messages will propagate into the network and resources will be misused because of excessive spurious traffic.

Fig. 5 is the pseudo code for detection of a relay node as an attacker. In our scheme ER (encounter record) table is maintained by all the nodes in which they include no of sent messages, message Id, sequence no and time stamp. They will also maintain a table for trust value of previously encountered nodes. Trust values also update transitively by recommendation of previously encountered nodes.

Node having no of sent messages less than the threshold L and its trust value greater than the initial value will be considered as a non-attacker node. Senders will continue to send messages to that node. Node having no. of sent messages greater than the threshold L and trust value greater than the initial value will become a suspect, but it will remain in the network as a second chance. If it continues to violate the threshold than that node is marked as an attacker node. Node having no of the sent messages greater than the threshold and trust value less than the initial trust than that node will immediately marked as an attacker node.

- **Detection of a Relay node as an attacker**

1. Allocate threshold L and initial trust T // L defines maximum allowed
2. **For each** Encounter
3. Exchange ER table //Encounter record table defines no. of sent. It consists of Message ID, Seq. No., and Time Stamp
4. **If** (no. of sent list ≥ L)
5. **If** (Trust ≥ Initial Trust)
6. Continue to send message
7. **Else**
8. Blacklist. Add (Node ID)
9. Inform Network about blacklisted node
10. **End If**
11. **End If**

Fig. 5 Detecting relay node as an attacker.

B. Detection of Sender node as an attacker

As shown in Fig.4 (a) when a sender or source node is an attacker they will forward replicas of self-generated genuine messages into the network. Thus, network is flooded by replica flooding.

Fig.6 is the pseudo code of detecting sender as an attacker. When a sender is an attacker or it is given a second chance in first phase than the receiving node will monitor the incoming messages coming from that node. If the no of copies are still exceeding the threshold value than the node is marked as an attacker node and its trust value is decremented.

If a sender is given a second chance in first phase than the receiving node will monitor the incoming messages coming from that node. If the number of copies is still exceeding the threshold value. Than the node is marked as an attacker node and its trust value is set to less than initial trust value.

- **Detection of Sender Node as an Attacker**

1. Allocate threshold L// L defines maximum allowed messes to send for every nodes
2. Set message Count to 0
3. Set timer to 0
4. **For** Last Meeting (contact duration)
5. Count Received Messages
6. **If** (message Count ≥L)
7. Blacklist .Add (Node ID)
8. Inform network about blacklisted Node
9. **End if**

Fig. 6 Detecting Sender node as an attacker.

C. Illustrative Example:

Here threshold for sent list is taken 10 which is derived from two times of optimal expected delay[21]. Each node maintains its own number of sent messages during last encounter and trust value of other previously encountered node and their sent list. When two nodes encounter each other they exchange their

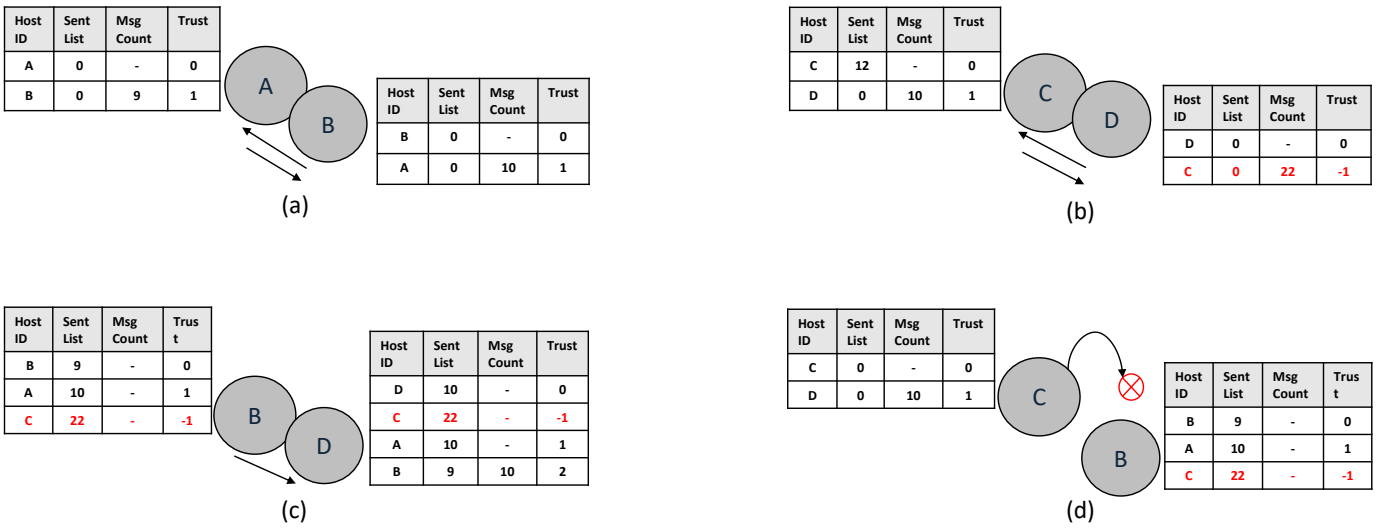

Fig. 7. Illustrative example of Proposed Scheme.

tables. Initial trust for all the nodes is 0. Here, as shown in Fig. 7. (a) node A and node B comes into each other's range. Initially both the nodes have not participated in message forwarding (when scenario starts). A will begin to send message to B. Node B will count incoming messages coming from node A which is 10. Msg count for node A is not exceeding the threshold so A's trust value will be incremented by 1 in B's table. At the same time node B will begin to send messages to A. Node A will aso count the incooming essages from B which is not exceeding the threshold so B's trust value is incremented by 1 in A's table. As shown in Fig. 7. (b) node C has its own no. of sent messages that is 12 > threshold (10), and its trust value is equal to initial trust. Node D will allow the node C to take part in communication once and sends messages to node C. Node D also examine msg count of node C (incoming messages from Node C). Message count of node C is now 22 > threshold(10). So now, D will black list the node C. As shown in Fig. 7. (c) When node D is encountered to node B both the nodes will exchange their tables. So, Node B is now aware of maliciousness of node C. Here only node B is willing to send messages to node D. Node D will check sentlist $\leq$ threshold and trust $\geq$ initial trust and start receiving messages from the node B and update the trust value accordingly. As schown in Fig. 7. (d) if blacklisted node C is encountered by node B. Node B will not communicate with that blacklisted node C because it is aware of the maliciousness of node C from node D's table.

V. Simulation Results and Analysis

A. Experimental Setup

Simulation shows that how the proposed scheme affects the network against various parameters. The simulation tool, ONE (Opportunistic Network Environment) is used to test the proposed scheme against the encounter record based existing scheme. Each node is having 10 Mb buffer size with the velocity of 0.5 ~1.5 m/s node velocity. Forwarding strategy of an individual attacker can vary from average attacker and very intense attacker based on that the results may be affected. We have varied number of attacker nodes from 4 to 12. Transmission speed and transmission range is varied from 100 kbps to 350 kbps and 40 meters to 120 meters respectively. The Binary Spray and Wait routing algorithm is used with L=10 where two times ED_{opt} is considered [12], [21]. The key simulation parameters are itemized in table1.

TABLE I
Simulation Parameters

Parameter	Values
Simulation Area	4500 x 3400
Simulation Time	43200 s
Buffer Size	10 Mb
Number of Nodes	126
Message Time to live	300 s
Transmit Speed	100 kbps-350kbps
Transmit Range	20 meters-100 meters
Number of attacker nodes	4-12
Mobility model	Shortest Path Based Mobility Model
Node Velocity	0.5 ~ 1.5 m/s
Number of Runs	10 Runs

B. Performance metrics

No. Of Dropped Messages: No. of dropped messages are total messages dropped during the simulation time. Flooding attack will cause a significant increase in dropped messages due to increase in spurious messages into the network.

Overhead Ratio: This metric shows the relayed minus delivered to delivered messages. Flooding attack will cause an increase in overhead ratio which should be decreased in a good scenario.

Latency Avg.: Network latency is an expression of how much time it takes for a packet of data to get from one designated point to another. We can consider the latency avg. in terms of average delay. Increase in spurious packets will cause delay in propagating the genuine packets resulting in higher latency.

Delivery Probability: It is defined as the fraction of packets delivered to their destinations out of all the unique packets generated. Delivery probability is ratio of delivered messages by created messages.

We have measured all this metrics against various network parameters as shown in Fig. 8, Fig. 9, Fig. 10 and Fig. 11.

C. Test 1: Varying No of Attacker nodes.

In this scenario, we vary the number of attacker nodes from 4 to 12 by keeping the transmission speed 250 kbps and transmission Range 100 meters. The buffer Size of the node is 10Mb. We consider two type of attackers by varying strategy of an individual attacker, one is generating average intensity of the flooding attack (i.e. Say a malicious node is multiplying each message by two rather dividing them by two in binary Spray and wait protocol) compared to the other higher intensity of flooding attack (i.e. Say a malicious node is multiplying each message by ten rather than dividing them by two as in binary Spry and wait Protocol). We call them flooding attack with average intensity and flooding with higher intensity respectively.

As shown in Fig. 8. (a) no. of dropped messages increases from 17086 to 33453 as the number of attacker increase in flooding attack. While in existing ER based scheme and proposed scheme gives significantly lower No. of dropped messages as flooding attack with average intensity is controlled by both the scheme. Fig. 8. (b) Shows that overhead ratio is increased from 12.6 to 26.17 in flooding attack while it is decreased in existing ER based scheme and proposed scheme. Fig. 8. (c) Shows higher delivery probability in proposed scheme as compared to attack and existing ER based scheme. Fig. 8. (d) Shows decreased latency of existing ER base scheme and proposed scheme while Fig. 9. Shows the higher intensity of flooding attack which cause significant changes in results of existing ER based scheme. Fig. 9. (a), (b), (c) and (d) Shows that in existing ER based scheme no. of dropped messages, overhead ratio and latency are significantly increased from 293201 to 316583, from 340.77 to 513.84 and from 1017.28 to 1061.83 respectively, and delivery probability is decreased from 0.59 to 0.42 as compared to the flooding attack (no. of dropped messages from 64682 to 226456, overhead ratio from 61.83 to 317.23 , latency 949.44 to 967.33 and delivery probability from 0.72 to 0.49) that proves the instability of ER based scheme against higher intensity of flooding attack. Whereas, proposed scheme is giving reduced no. of dropped

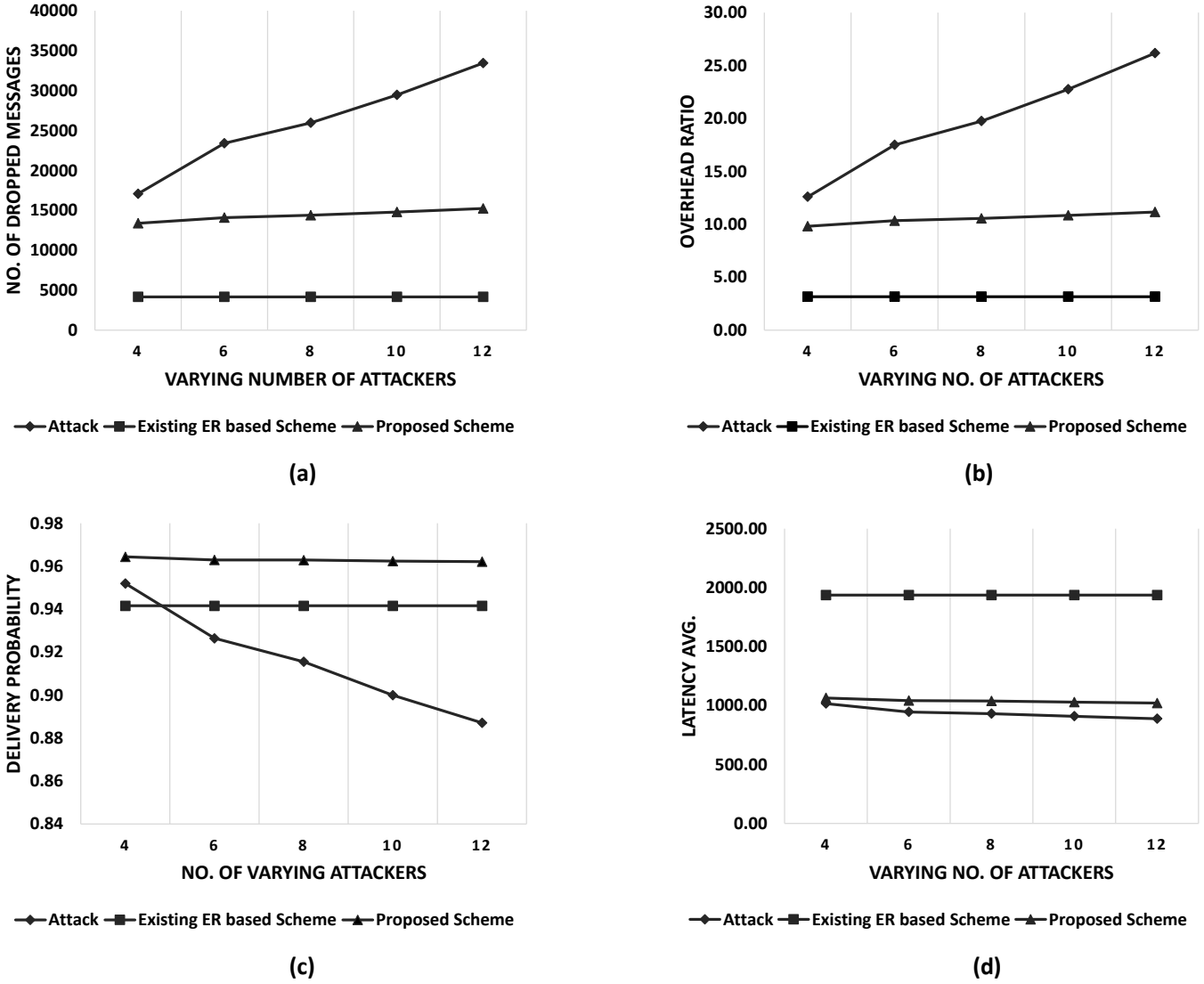

Fig. 8. Varying No of attacker under Average Intensity Flooding Attack. (a) No. of Dropped Messages, (b) Overhead Ratio, (c) Delivery Probability, (d) Latency average.

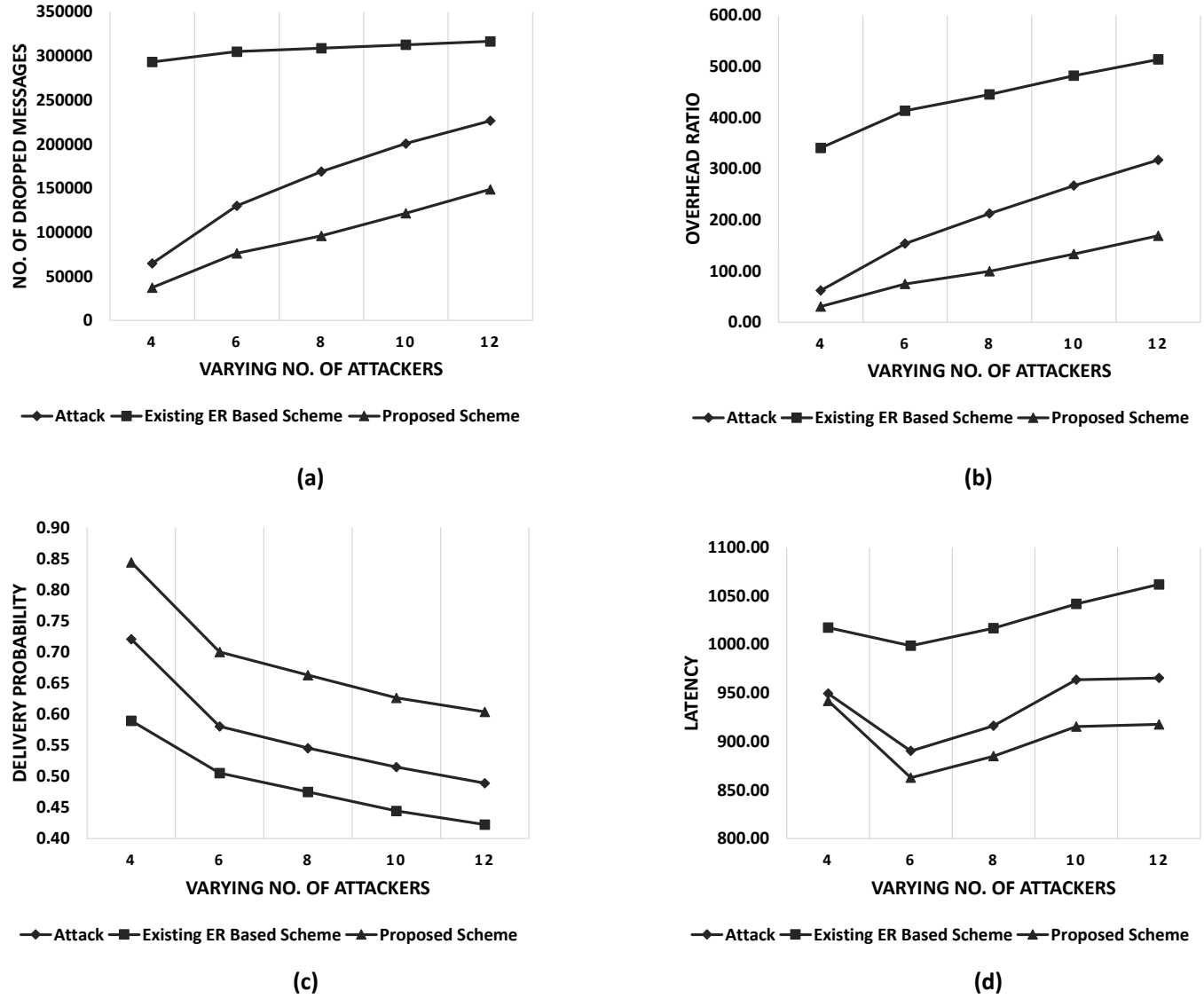

Fig. 9. Varying No of attacker under High Intensity Flooding Attack. (a) No. of Dropped Messages, (b) Overhead Ratio, (c) Delivery Probability, (d) Latency average.

messages from 37217 to 148705, overhead ratio from 30.51 to 168.89 and latency from 941.88 to 917.65, and increased delivery probability from 0.84 to 0.60 as compared to flooding attack and existing ER based scheme. These results demonstrates that proposed scheme is worth beneficial to fight against the flooding attack and gives batter network performance. Another aspect we observe here is that as shown in Fig. 9. (a), (b) and (c) as the number of attacker increases the no. of dropped messages and overhead ratio increases while the delivery probability is decreased because of the impact of malicious nodes. Now, we will conduct remaining two tests under higher intensity of flooding attack.

D. Test 2: Varying Transmit Speed.

In this scenario, we vary transmission speed from 100 to 350 by keeping the transmission range 100 meters and buffer size 10Mb. As shown in Fig. 10. (a) In flooding attack number of dropped messages are increased from 130630.8 to 250748.6, in existing ER based scheme the number of dropped messages increased as compared to flooding attack and in proposed scheme no. of dropped messages are decreased from 113258.3 to151534.8. As shown in Fig. 10. (b) Overhead ratio, in existing ER based scheme is increased from 285.93086 to 612.94498 while in proposed scheme, overhead ratio is decreased from 132.10942 to 173.27063. While increasing the transmission speed, the dropped messages and overhead ratio are increased because the nodes will be able to transfer more messages in their contact duration. As shown in Fig. 10. (c) Delivery probability, in existing ER based scheme is decreased from 0.39241 to 0.43943 while in proposed scheme delivery probability is increased from 0.58852 to 0.60012. As shown in Fig. 10. (d) Shows significantly decreased latency average in proposed scheme from 1113.2 to 910 as compared to existing ER based scheme (from 1743.2 to 990.4) and flooding attack (from 1251.25 to 987.1). Here increasing transmission speed will cause a decreased latency average because the transmission will speed up and delay of receiving a message at the destination is decreased. This test is conducted over higher

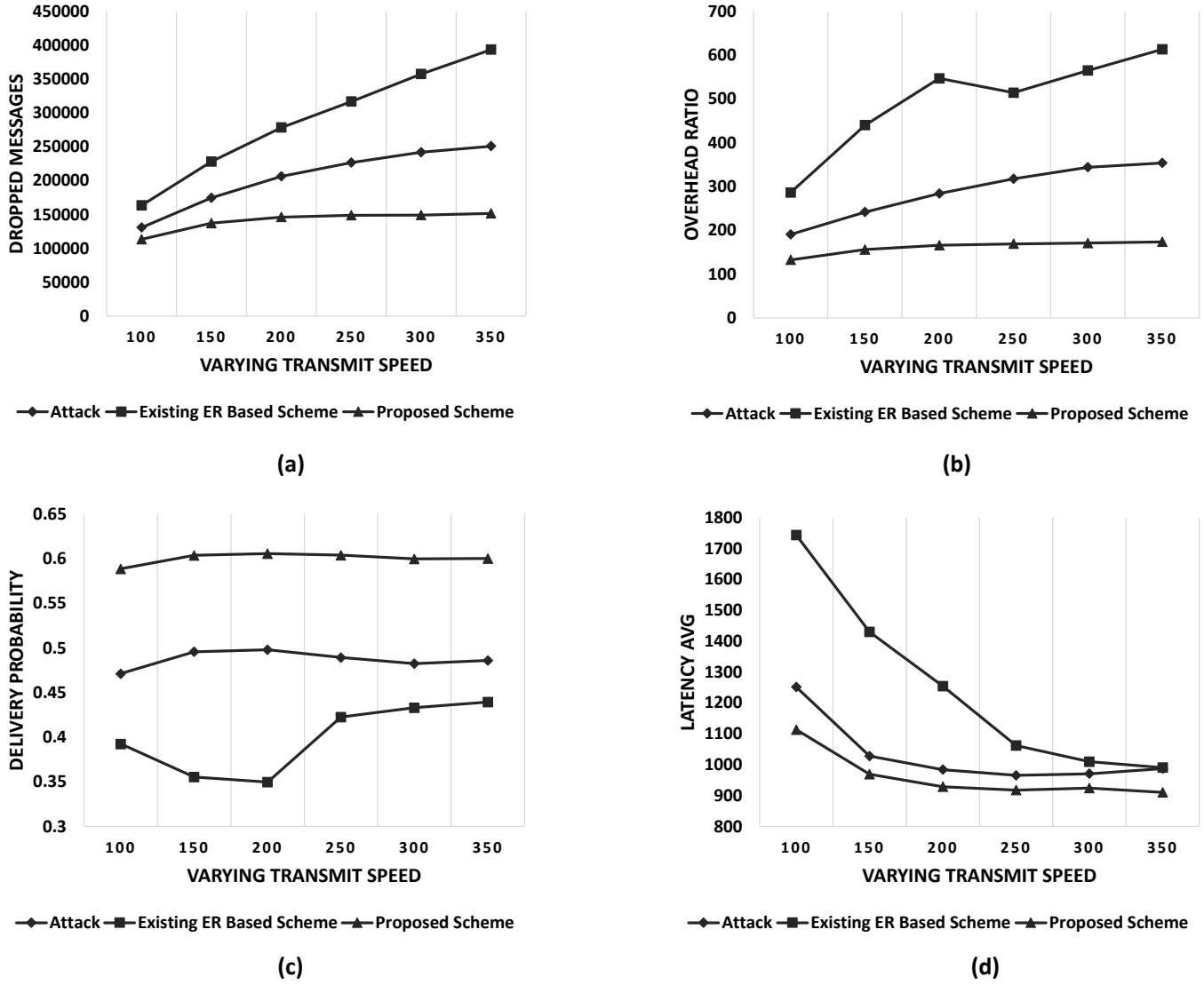

Fig. 10. Varying Transmit Speed under High Intensity Flooding Attack. (a) No. of Dropped Messages, (b) Overhead Ratio, (c) Delivery Probability, (d) Latency average.

intensity of flooding attack which is decided by the forwarding strategy of an individual attacker. Simulation results shows that the proposed scheme is giving batter results as compared to existing ER record based scheme.

E. Test 3: Varying Transmit Range.

In this scenario, we vary the transmission range from 40 meters to 120 meters by keeping transmission speed 250 kbps and buffer size 10Mb. As shown in Fig. 11. (a) In existing ER based scheme no. of dropped messages are increased from 162037.9 to 371503.8, In flooding attack no. of dropped messages are increased from 128232.8 to 257404.4 while proposed scheme is giving less number of dropped messages from 103913 to 157067 as compared to flooding attack and existing ER based scheme while increasing the value of transmission range. As shown in Fig. 11. (b) In flooding attack overhead ratio is increased from 223.1 to 352.9. In existing ER based scheme overhead ratio is increased from 296.52 to 562.38 while proposed scheme gives less overhead from 130.8 to 173.8 while increasing the value of transmission range. As shown in Fig. 11. (c), in flooding attack and in existing ER based scheme delivery probability is lower from 0.39835 to 0.49973 and from 0.37479 to 0.45235 respectively. While the proposed scheme is giving higher delivery probability from 0.54599 to 0.61995. As shown in Fig. 11. (d) Flooding attack and existing ER based scheme gives higher latency from 1521.79 to 899.41 and from 1969 to 939.6 respectively. Proposed scheme gives quiet lower latency from 1320.4 to 851.7 while increasing the transmit range from 40 to 120.

VI. CONCLUSION

Security in DTN has been a crucial issue to be addressed. In this paper, we have studied the effects of *replica flooding attack* on the network performance when the nodes follow *Binary Spray and Wait* protocol. The malicious nodes may disrupt the forwarding strategy and insert spurious replicas of genuine

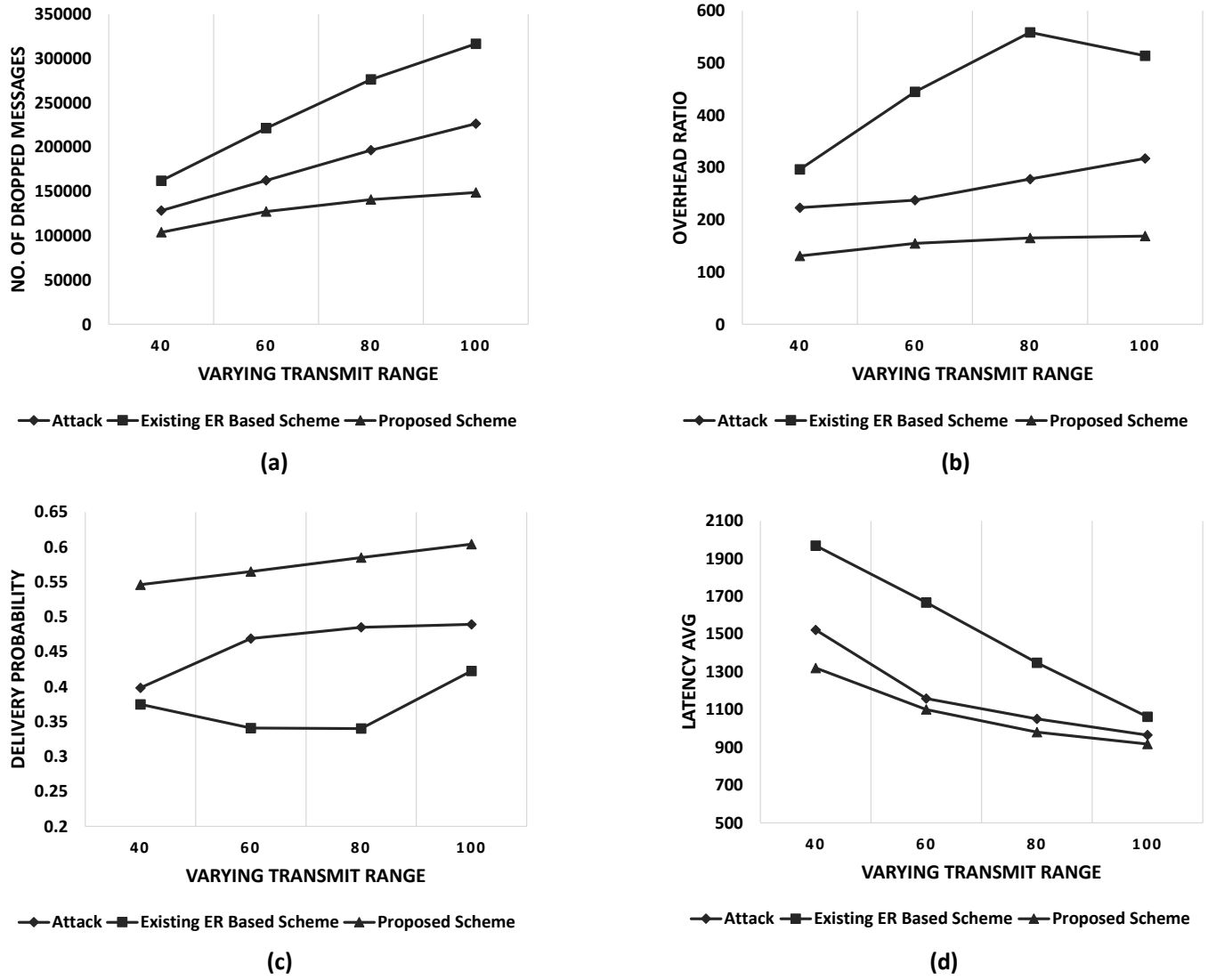

Fig. 11. Varying Transmit Range under High Intensity Flooding Attack. (a) No. of Dropped Messages, (b) Overhead Ratio, (c) Delivery Probability, (d) Latency average.

packets into the network. We address this issue by combining the Existing ER Based Scheme with the Trust-based scheme. Our Scheme is divided into two parts: Detecting Sender as an Adversary and Detecting Receiver as an Adversary. A trust metric is used along with SL of the node to measure trustworthiness of the node. Simulation results are carried out by varying various network parameters to measure the network performance under high load and initial average load. We conclude that the existing ER based scheme is giving good performance at initial stage of flooding attack. High intensity flooding attack cause the existing ER based strategy to degrade the network performance. Whereas, the proposed scheme gives better network performance even with high load caused by the attack. The proposed scheme results in less number of dropped messages, overhead ratio, latency, and increased delivery probability of the message.

REFERENCES

[1] S. K. Das Sujoy Saha, Subrata Nandi,Rohit Verma,Satadal Sengupta,Kartikeya Singh,Vivek Sinha, “Design of efficient lightweight strategies to combat DoS attack in delay tolerant network routing.pdf.” 2016.

[2] H. Guo, X. Wang, H. Cheng, and M. Huang, “A routing defense mechanism using evolutionary game theory for Delay Tolerant Networks,” *Appl. Soft Comput.*, vol. 38, pp. 469–476, 2016.

[3] A. K. Gupta, I. Bhattacharya, P. S. Banerjee, J. K. Mandal, and A. Mukherjee, “DirMove: direction of movement based routing in DTN architecture for post-disaster scenario,” *Wirel. Networks*, vol. 22, no. 3, pp. 723–740, 2016.

[4] C. Chakrabarti and S. Roy, “An Observer based Distributed Scheme for Selfish node Detection in

Post-disaster Communication Environment using Delay Tolerant Network."

[5] J. Zhou, M. Song, J. Song, X. W. Zhou, and L. Sun, "Autonomic group key management in deep space DTN," *Wirel. Pers. Commun.*, vol. 77, no. 1, pp. 269–287, 2014.

[6] X. Lv, Y. Mu, and H. Li, "Loss-Tolerant Bundle Fragment Authentication for Space-Based DTNs," *IEEE Trans. Dependable Secur. Comput.*, vol. 12, no. 6, pp. 615–625, 2015.

[7] X. Lv, Y. Mu, and H. Li, "Non-interactive key establishment for bundle security protocol of space DTNs," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 1, pp. 5–13, 2014.

[8] H. L. Xixiang LV, "Error- and loss-tolerant bundle fragment authentication for space DTNs," vol. 8, no. 6, pp. 1012–1023, 2014.

[9] P. Puri and M. P. Singh, "A survey paper on routing in delay-tolerant networks," *Proc. 2013 Int. Conf. Inf. Syst. Comput. Networks, ISCON 2013*, pp. 215–220, 2013.

[10] A. Fatimah and R. Johari, "Part: Performance Analysis of Routing Techniques in Delay Tolerant Network," *Proc. Int. Conf. Internet Things Cloud Comput.*, pp. 76:1–76:5, 2016.

[11] Y. Guo, S. Schildt, T. Pogel, and L. Wolf, "Detecting malicious behavior in a vehicular DTN for public transportation," *Glob. Inf. Infrastruct. Symp. GIIS 2013*, 2013.

[12] P. Thi and N. Diep, "Detecting Flooding Attack in Delay Tolerant Networks by Piggybacking Encounter Records," 2015.

[13] H. Chen, W. Lou, Z. Wang, and Q. Wang, "A Secure Credit-Based Incentive Mechanism for Message Forwarding in Noncooperative DTNs," *IEEE Trans. Veh. Technol.*, vol. 9545, no. c, pp. 1–1, 2015.

[14] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 6, pp. 1299–1314, 2015.

[15] G. Ansa, H. Criuckshank, Z. Sun, and M. Al-siyabi, "A DOS-Resilient Design for Delay Tolerant Networks," pp. 424–429, 2011.

[16] Q. Li, W. Gao, S. Zhu, and G. Cao, "To lie or to comply: Defending against flood attacks in disruption tolerant networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 10, no. 3, pp. 168–182, 2013.

[17] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," *Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous 2007*. 2007.

[18] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "MUTON: Detecting malicious nodes in disruption-tolerant networks," *IEEE Wireless Communications and Networking Conference, WCNC*. 2010.

[19] D. Bucur, G. Iacca, M. Gaudesi, G. Squillero, and A. Tonda, "Optimizing groups of colluding strong attackers in mobile urban communication networks with evolutionary algorithms ☪," *Appl. Soft Comput. J.*, vol. 40, pp. 416–426, 2016.

[20] F. C. Lee, W. Goh, and C. K. Yeo, "A Queuing Mechanism to Alleviate Flooding Attacks in Probabilistic Delay Tolerant Networks," pp. 329–334, 2010.

[21] C. S. Raghavendra, "Spray and Wait : An Efficient Routing Scheme for."