Mitigating Blackhole Attacks in Delay Tolerant Networks

Aysha Al Hinai, Haibo Zhang and Yawen Chen
Department of Computer Science, University of Otago, New Zealand
{aalhinai, haibo, yawen}@cs.otago.ac.nz

***Abstract*—Unlike the conventional routing techniques in the Internet where routing privileges are given to trustworthy and fully authenticated nodes, Delay Tolerant Networks (DTNs) allow any node to participate in routing due to the lack of consistent infrastructure and central administration. This creates new security challenges as even authorized nodes in DTNs could inject several malicious threats against the network. This paper investigates novel solutions based on the Spray-and-Wait (SnW) routing protocol for mitigating blackhole attacks in DTNs. A new knowledge-based routing scheme, called Trust-Based Spray-and-Wait protocol (TB-SnW), is proposed. The routing decisions in TB-SnW protocol are made based on the trust levels that are computed at each node using its historic routing records. Simulation results show that the TB-SnW protocol can achieve better performance in terms of mitigating Byzantine attacks and reducing message delivery delay compared with the Spray-and-Wait protocol.**

***Index Terms*—Routing, DTN, Byzantine Attacks, Trust Measurement**

I. Introduction

Delay Tolerant Networks (DTNs) is a class of networks that represents one of the major areas in the field of wireless networking [1]. Communications in DTNs can be characterized as opportunistic point-to-point transmission from sources to destinations. The opportunistic feature means that there is no specific scheduled time in which a message must be forwarded, and end-to-end communication is not practical due to the intermittent contact between the communicating nodes. DTNs have a wide range of applications such as providing internet services in rural areas [2], wildlife tracking [3], sensor networks [4] and interplanetary internet [5].

Due to the lack of end-to-end communication, conventional routing schemes based on single-copy forwarding cannot work in DTNs with highly unstable network topology. They cannot guarantee sufficient robustness in the very sparse DTN environment because the single custodian node can be down at any time and the single copy can simply be lost. Flooding-based routing is entirely opposite to the single copy forwarding-based routing scheme. Epidemic router [6] is a typical example of flooding-based routers. A node applying flooding-based routing protocols sends a replica of each message to any node it encounters. Thus, the number of replicas of a message in flooding-based protocols is dependent on the scope of the network. In large scale networks, this leads to extensive consumption of a limited resources, causing significant overhead. Flooding-based protocols are one branch of *Replication-based* routing [7], where *quota-based* routing [7] is the other branch. Quota-based routers initially limit the number of copies per message to avoid the excessive usage of the network resources and to eliminate extra overhead. The Spray-and-wait router (SnW) [8] is one example of quota-based implementation which will be discussed in Section III.

Communications in DTNs are highly susceptible to various kinds of attacks since adversaries in that networks can exhibit malicious actions to negatively degrade the network's performance. Their actions can vary from tampering with the message content, to fraudulently redirecting the messages, flooding the network with unnecessary data, or even blindly dropping messages in transit. These activities can threaten the data integrity, confidentiality, network availability and data delivery. Encounter-based Protocols [7] are another category of DTN routing protocols. The encounter-based router (EBR) makes routing decisions based on past encountering states. It takes advantage of the mobility feature of nodes in DTNs in which future encounter probability can be predicted from past mobility trends. In EBR the larger the past encounter rate, the higher the potential of successful message delivery. So routing decision in EBR are made according to the encounter rate between two nodes. EBR suffers from a major security breach because attackers can easily modify their movement pattern in order to gain higher encounter rate and hence grab the chance of being an intermediate node, which will cause a blackhole or exhibit any other adversarial behavior in the network.

Our main objective in this paper is to measure the impact of malicious byzantine behavior on the performance of DTNs and propose an efficient mitigation mechanism. This is achieved by investigating the impact of a blackhole attack in a DTN using Spray and Wait router. The main contributions of this work includes:

- We evaluate the performance of Spray-and-Wait routing protocol in networks with blackhole attacks. Simulation results show that blackhole attacks can significantly reduce message delivery rate, increasing the average message delivery latency.
- We propose a new protocol, called Trust-Based Spray-and-Wait (TB-SnW), based on trust management. The basic idea of the protocol is to let each node maintain a trust list for all other nodes it meets, and use the trust level to mitigate attacks.
- We evaluate our proposed protocol in simulations by

comparing it with the Spray-and-Wait protocol. Simulation results demonstrate that TB-SnW can achieve a higher message delivery rate than Spray-and-Wait. Moreover, it does not introduce too much overhead to the network.

The rest of this paper is organized as follows. Section II gives background and related work about the security issues in DTNs. Section III describes the Spray and Wait routing protocol. Then Section IV evaluates the performance of Spray and Wait routing protocol in the existence of blackhole attacks. In Section V we describe our proposed mitigation scheme, and compare it with Spray and Wait router in Section VI. Finally we conclude our paper and discuss the future work in Section VII.

II. Background and Related Work

A. Blackhole Attacks in DTN

Authenticating before participating is highly recommended in any kind of network protocol. This is to ensure that the messages generated by each node are trustworthy. Even though a node is authorized according to the protocols, there is no guarantee that all of its actions will be legitimate. The attack in which an adversary user is authorized to access the network resources and performs any action to disrupt its network is referred to as the Byzantine attack [4]. Blackhole attack is one class of Byzantine attacks. In a blackhole attack, the adversary node advertises itself as honest, where it has the intention of intercepting messages, preventing them from reaching their destinations. It is similar to the black-hole of the universe because they both cause things to disappear.

B. Related Work

Although most of the routing protocols designed for DTNs focus on secure routing, many of them cannot address byzantine attacks that result from compromised nodes within the network. The approach proposed in [9] takes advantage of the ability of nodes to overhear the traffic generated by other nodes to detect the abnormal behavior of their neighbors. In practice, this mechanism is not that effective as nodes in DTNs can be sparsely scattered and nodes might not be able to overhear others due to long distance and limited transmission range. In [10] [11], blackhole detection is done by specific third-party nodes called *ferries*. Ferry nodes move around the network and examine the delivery probabilities[1] to determine the existence of a blackhole attack. Unfortunately, if the ferries are compromised, it will cause a major threat in the network. To avoid this issue, TB-SnW preforms a clever distributed blackhole detection and trust management in which each node examines the trust level of each node it wants to use as a next relay and decides whether that node is trustworthy or an adversary. This can provide faster adversary detection without the need for third-party nodes to do this job.

[1]Delivery predictability is a forwarding metric used by PRoPHET router. Nodes with higher delivery predictability have higher potential to forward messages to a node compared with nodes with lower delivery predictability.

III. The Spray-and-Wait Routing Protocol

The Spray-and-Wait (SnW) routing protocol [8] is a representative replication-based routing protocol designed for DTNs. Unlike the conventional routing schemes, it allows a node to forward more than one copy for each message to different nodes, thereby increasing the message delivery rate. Unlike flooding-based routing protocols, it not only imposes a bound on the total number of copies and transmissions per message without compromising performance, but also constrains the number of forwarders that are allowed to forward each message, thus not introducing too much communication overhead to the network. Simulation results show that: (i) under low load, SnW results in much fewer transmissions and comparable or smaller delays than flooding-based schemes, (ii) under high load, it yields significantly shorter delays and fewer transmissions than flooding-based schemes.

SnW works in two phases: *Spray phase* and *Wait phase*. In the spray phase, for every message originating at a source node, a fixed number of message copies are initially spread by the source and possibly received by other nodes. In the wait phase, if the destination is not found in the spraying phase, each node that carries only one message copy performs direct transmission (i.e. will forward the message only to its destination). SnW can work in two modes: the *Normal Mode* and the *Binary Mode*, according to the number of replicas a node can forward to another node. In the Normal Mode, a node forwards a single copy of the message to any other node it encounters. In the Binary Mode, the sender transfers half of the copies it is holding to any node it meets. When a node gives away all the message replicas, except the one left for itself, it switches to the waiting phase in which it will keep that replica until it is in direct contact with the final destination.

Obviously, SnW routing protocol can increase the potential of successful message delivery in a normal network environment that is free from attacks. But how about a network that its susceptible to various kinds of attacks? In the subsequent section, we will carry out simulations to evaluate the performance with adversarial attacks.

IV. Spray-and-Wait Under Blackhole Attacks

To evaluate the performance of the SnW protocol in a network that suffers from intrusive behaviors, we carried out a set of simulations in the *Opportunistic Network Environment simulator* (ONE) [12], which is especially designed for simulating DTNs. In our simulation, 125 mobile nodes are scattered over the map of of Helsinki City (the default map in the ONE simulator), and divided into six groups. Each group has different configurations for radio range, node moving speed, buffer size and so on. Each node is associated with a probability with which the node will behave like a blackhole attacker. For example, if a node behaves as an attacker with probability p, it will drop every message it receives with probability p. In our simulation, we configure all nodes with the same probability p, and vary p to evaluate the performance of the SnW protocol under different degrees of blackhole attack. Each node generates 10 replicas of each message it

creates and spreads them to the other forwarding nodes or destination. For each setting of p, the simulation is run for five hours.

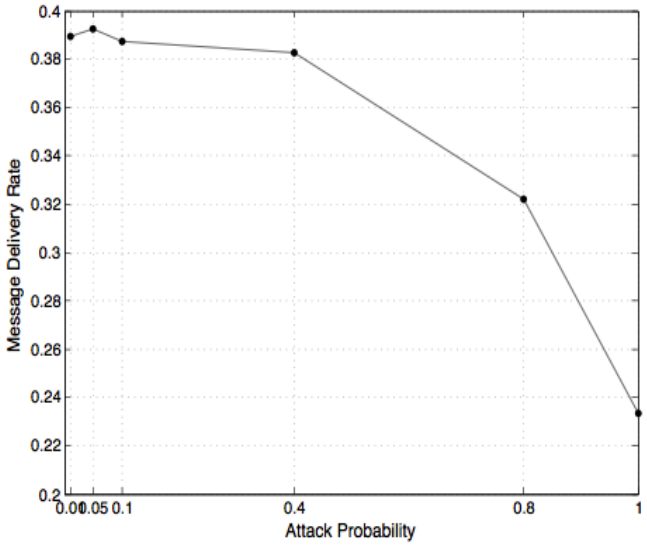

Fig. 1. Impact of Blackhole Attacks on message delivery rate

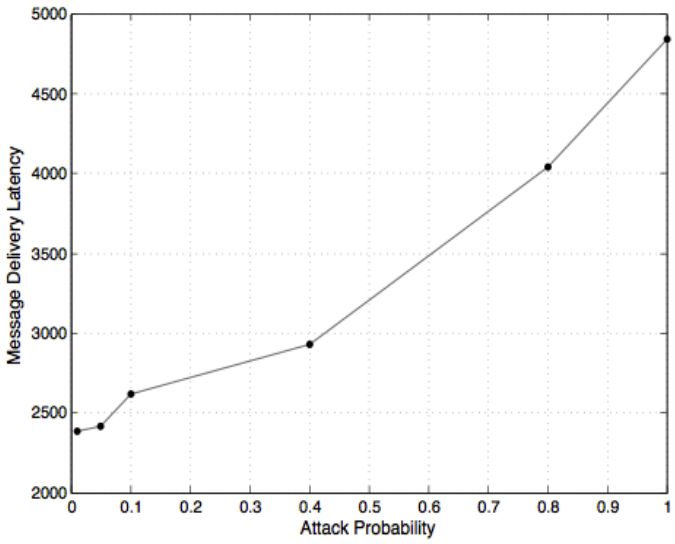

Fig. 2. Impact of Blackhole Attacks on message delivery delay

Figure 1 shows the impact of blackhole attack on the overall message delivery rate. It can be seen that the message delivery rate only slightly increases when p is increased from 0 to 0.4. This is because each node will generate 10 replicas for each message it generates, and the delivery is successful as long as there is one replica that arrives at the destination. With the further increasing of p, the message delivery rate decreases significantly. It is worth noting that when the attack probability was 1 the delivery rate dropped to 0.235. This indicates that all successfully delivered packets are directly transmitted from sources to the destinations without any use of intermediate nodes, as they are all attackers.

Another critical metric we need to consider is the impact of attack probability p on the message delivery latency (measured in seconds), which is defined as the time needed for a message to be successfully received by its final destination [4]. As shown in Figure 2, increasing attack probability increases the delivery latency. This is because when the number of attackers in the network increases, more messages get dropped, and each destination has to wait for a longer time till one copy of message can manage to survive and reach the destination.

It can be seen from the above simulation results that the SnW protocol is not resistant to blackhole attacks, especially when the number of attackers in the network is high. In the following section we will propose an enhanced SnW protocol based on trust management to mitigate blackhole attacks.

V. Trust-based Spray and Wait Protocol

To countermeasure attacks in DTNs, an honest node generally takes the following two measures: (1) choosing not to remove messages from its buffer upon delivery, and (2) creating more message replicas. Both approaches have the disadvantages of overburdening the network with too many message copies, resulting in network congestion and longer message delivery delay. In this section we introduce a new routing scheme called Trust-Based Spray and Wait (henceforth referred to as TB-SnW) for detecting and mitigating blackhole attacks. The basic idea of TB-SnW is to maintain a list of forwarders in the local memory of each node, and dynamically update the trust level for each forwarder in the list based on the transmission history. Using the trust level, each node can intelligently distribute the replicas to other forwarders. The higher the trust level a forwarder has, the more replicas will be sent to it. This scheme can counteract blackhole attack without overwhelming the network with replicated messages.

The TB-SnW protocol is composed of two components: (1) trust measurement component that is responsible for maintaining the list of next-hop forwarders, and the trust level for each next-hop forwarder; (2) replica distribution component that is responsible for wisely distributing the replicas to the next-hop forwarders.

A. Trust Measurement Component

In DTNs it is not feasible to build a central trust management system as the network state is changing over time. Therefore, the TB-SnW protocol builds a distributed trust management mechanism by which each node in the network establishes and maintains a local trust database called trust list. Each entry in the trust list has two fields: host-ID and M-Count. The host-ID records the identification of the node from which the current node has successfully received messages, whereas the M-Count records the number of messages that are received from the node with that host-ID. We use an ArrayList data-structure to store the host-ID and M-Count information locally at each node. This information is not allowed to be transferred to or used by any other node in the network in

order to eliminate the possibility of introducing new attacks by exploiting this list.

B. Replica Distribution Component

The basic idea of TB-SnW is to smartly distribute the message replicas based on the forwarders' trust levels. The higher the trust level a forwarder has, the more the number of replicas it should receive. Let λ be a user-defined threshold for the trust level. If the M-count value for a forwarder is larger than λ, the node is treated as a trust-worthy node. Given any node i which holds n replicas for a message, it will perform one of the following three operations based on n and λ when it meets another node j.

1) If $n = 1$, node i will not spread the only copy it holds, and goes into wait phase.
2) If $n > 1$ and node j is not a trustworthy forwarder, node i will forward only one replica to node j. This is because, if a node's trust level is below the threshold, it does not necessarily mean that it is a blackhole attacker. This might be due to disconnection during transaction or inadequate buffer size.
3) If $n > 1$ and node j is a trustworthy forwarder, the number of replicas that node i should forward to node j, denoted by $R_{i,j}$, is computed using the following equation:

$$R_{i,j} = \begin{cases} n - n_f - 1, & x > n - n_f - 1, \\ x = \lceil (n-1) \times \frac{m_{i,j}}{\sum_{k=0}^{L} m_{i,k}} \rceil, & x \leq n - n_f - 1. \end{cases}$$

where $m_{i,j}$ is the M-Count value for node j stored in node i's trust list, L is the number of forwarders stored in node i's trust list, and n_f is the number of replicas that has already been spread. $R_{i,j}$ should not be larger than $n - n_f - 1$ since it needs to keep a replica for itself.

VI. Performance Evaluation

In this section, we evaluate the performance of the designed TB-SnW protocol through simulations in the ONE simulator in comparison with the Spray-and-Way protocol. We use the same simulation setup as described in Section IV except the configuration of blackhole attackers. In Section IV we implemented a method to choose nodes to behave as blackhole attackers with some probability. But this method is not applicable to evaluate TB-SnW because it requires the trust level of each node. In order to measure the performance of TB-SnW during an attack, we need to introduce a specific non-random set of nodes to perform intentional message dropping attacks. In our simulations, the set of attackers are chosen from different groups with different capabilities, such as pedestrians, cars and trams, to simulate real-life interactions.

A. Impact of the Trust Threshold

In this set of simulations, we vary the trust threshold to evaluate the performance of TB-SnW. Trust threshold is a key factor to consider when building any trust relationship in TB-SnW. Choosing an optimal threshold value is essential to safeguard routing and communication in DTNs. If the threshold value is chosen to be extremely high the TB-SnW performance will reach a similar level to the normal mode of SnW because the number of messages to be forwarded will be one in most cases. The threshold value should not be low, because a high amount of copies will be transferred to nodes that are not very trustworthy. As can be seen from Figure 3 and Figure 4, both the delivery rate and the overhead ratio remains roughly stable when increasing the trust threshold from 4 to 14, and the minimum average latency is also achieved when setting the trust threshold to 4. Therefore, to gain the best routing efficiency, the threshold value should be optimal.

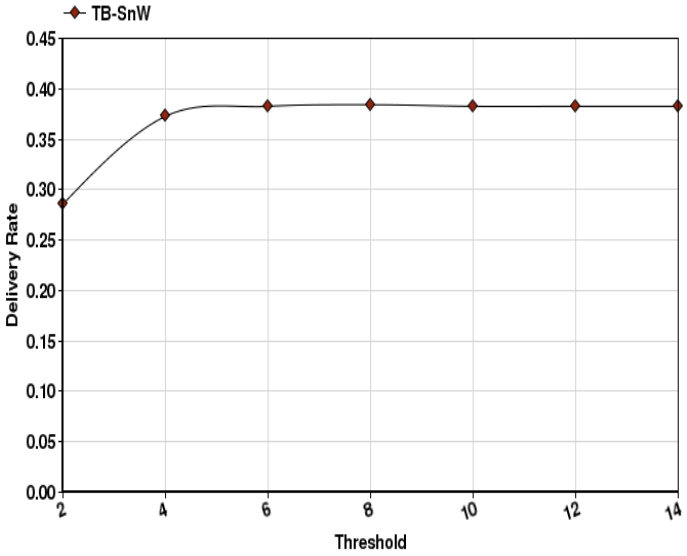

Fig. 3. Delivery rate under different thresholds

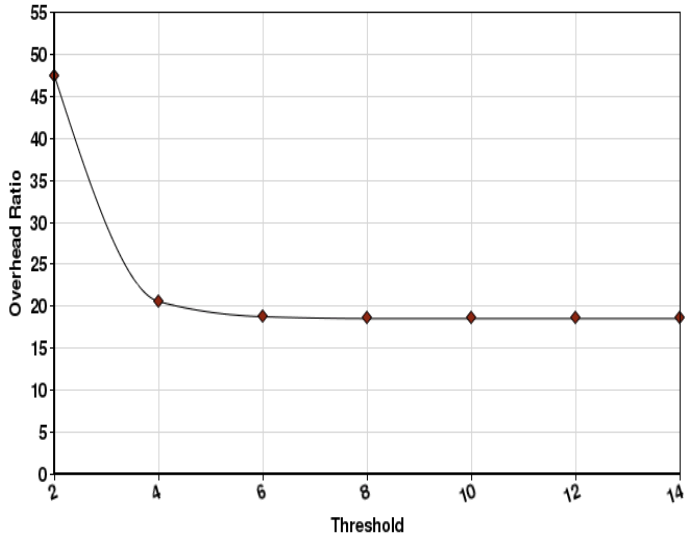

Fig. 4. Overhead under different thresholds

B. Impact of the Number of Message Copies

In this set of simulations, the simulation time is configured to run for 5 hours, the number of attackers is set to 8, and the

threshold λ is set to be 8. We compare TB-SnW with SnW operating in normal mode. Figure 5 shows the comparison for the message delivery rate under different configurations of the number of replicas. We can see that the performance of TB-SnW is better than that of the SnW protocol in all cases studied. When the number of replicas is set to 5, the delivery rate of TB-SnW is 20.22% higher than that of SnW. There is no doubt that increasing the message copies when there is no attack will increase the message delivery rate because it increases the probability that at least one copy can travel through a shorter path.

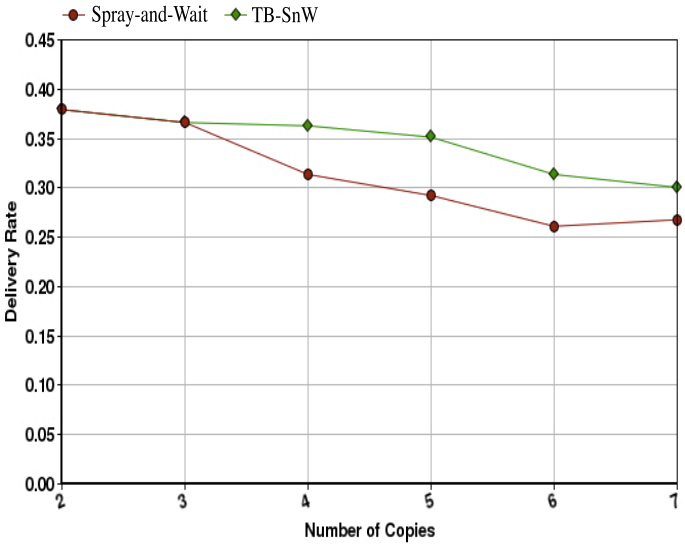

Fig. 5. Message delivery rate with different number of replicas

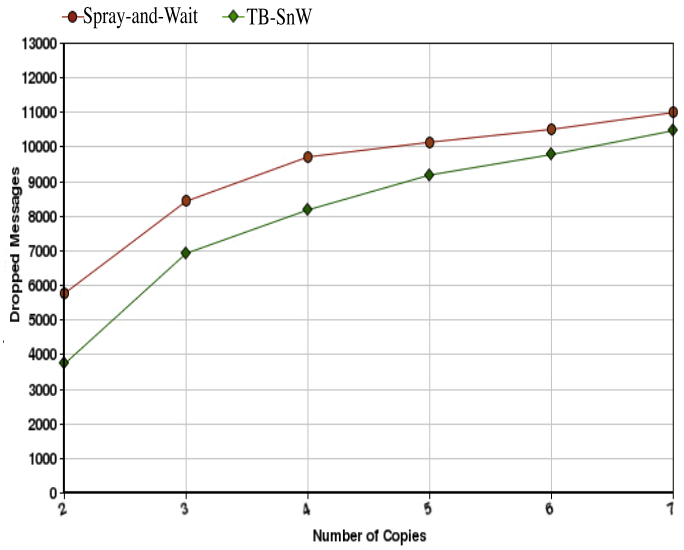

Fig. 6. Message dropping rate with different number of replicas

But surprisingly, in networks with blackhole attacks, increasing the number of replicas does not increase the message delivery rate. This phenomenon can be explained using the message dropping rate plotted in Figure 6. A message can be dropped due to three reasons: (1) limited buffer capacity; (2) very frequent disconnections when transiting message; and (3) blackhole attacks. It can be seen that blackhole attacks have a great impact on the message dropping rate. The more replicas we inject into the network, the more messages will be forwarded to the blackhole attackers and get dropped. Compared with SnW protocol, TB-SnW showed higher efficiency to mitigate the attack by having less number of dropped messages than SnW. For instance, the difference of message loss percentage when two copies are used is up to 35.35%.

Figure 7 compares the average message delivery latency in TB-SnW and SnW protocols. TB-SnW tends to show faster message delivery than SnW in most cases. This results from choosing more reliable forwarders that makes most replicas go to trusty nodes.

As illustrated in Figure 8 the network overhead gradually raises if the message copies increase. This is true in DTNs no matter if the network is free from blackholes or it suffers from that attack. In addition, the routing overhead of a DTN using normal SnW is visibly much higher than TB-SnW. From the simulation statistics we can see that TB-SnW can reduce the overhead up to 27.12% in comparison with the SnW when the number of copies is set to 4.

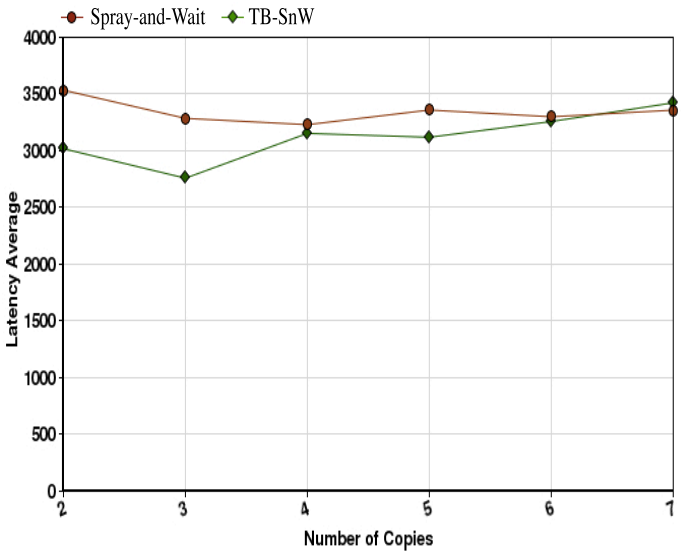

Fig. 7. The average message delivery latency with different number of replicas

VII. Conclusion and Future Work

In this paper, we proposed a new trust-based routing framework, TB-SnW protocol, that can efficiently avoid the blackhole threat. Our proposed TB-SnW protocol introduces a distributed trust management method to facilitate node authentication in an environment that cannot apply central administration. In order to distinguish the honest ones from blackholes, TB-SnW takes advantage of the previous behavior of nodes, and provides a wise dynamic mechanism to

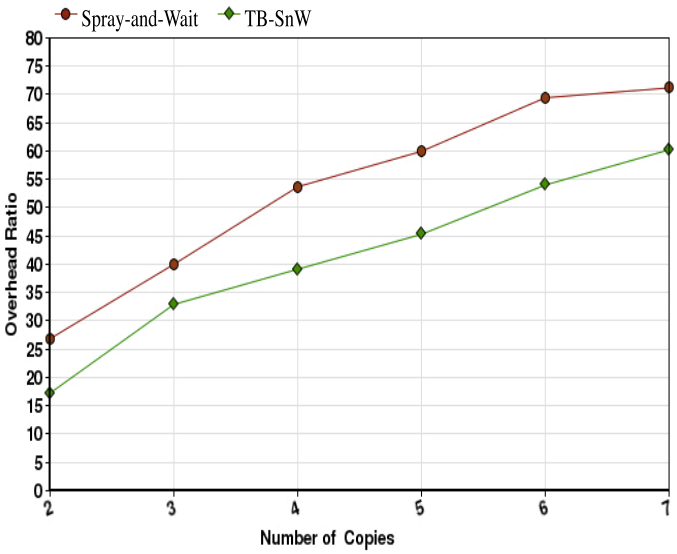

Fig. 8. Overhead Ratio Comparison

assign replicas to nodes. By using the trust-based message forwarding scheme, TB-SnW protocol can improve the DTNs' performance and can provide better handling with security threat than conventional SnW. Our performance evaluation shows that TB-SnW can achieve a higher level of delivery rate because of its ability to maintain lower dropping rate. Furthermore, TB-SnW produces lower network overhead compared with the conventional SnW.

An interesting future work is that TB-SnW can be further combined with other byzantine attacks mitigation schemes to produce a routing protocol that is ready to defeat various kinds of potential attacks caused by compromised nodes.

REFERENCES

[1] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM '03, 2003.

[2] A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, "Low-cost communication for rural internet kiosks using mechanical backhaul," in *Proceedings of the 12th annual international conference on Mobile computing and networking*, ser. MobiCom '06. New York, NY, USA: ACM, 2006, pp. 334–345.

[3] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet," *SIGPLAN Not.*, vol. 37, pp. 96–107, October 2002. [Online]. Available: http://doi.acm.org/10.1145/605432.605408

[4] M. Karimzadeh, "Efficient routing protocol in delay tolerant networks (DTNs)," Master's thesis, Tampereen teknillinen yliopisto, 2011.

[5] S. Farrell, V. Cahill, D. Geraghty, I. Humphreys, and P. McDonald, "When TCP breaks: Delay- and disruption- tolerant networking," *IEEE Internet Computing*, vol. 10, pp. 72–78, 2006.

[6] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Department ofComputer Science, Duke University, Tech. Rep., 2000.

[7] S. C. Nelson, M. Bakht, and R. Kravets, "Encounter-based routing in DTNs," Department of Computer Science University of Illinois at Urbana-Champaign, Tech. Rep.

[8] S. Thrasyvoulos, P. Konstantinos, and R. C. S, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, 2005, pp. 252–259.

[9] Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, New York, NY, USA, 2003, pp. 135–147. [Online]. Available: http://doi.acm.org/10.1145/986858.986877

[10] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," in *Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MobiQuitous)*, ser. MOBIQUITOUS '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 1–8.

[11] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Muton: Detecting malicious nodes in disruption-tolerant networks," in *WCNC'10*, 2010, pp. 1–6.

[12] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE Simulator for DTN Protocol Evaluation," in *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. New York, NY, USA: ICST, 2009.