Node Cooperation Strategy on Security Aided and Group Encounter Prophet Routing Protocol of an Opportunistic Network

H. J. Abubakar
Electrical and Computer Engineering Department, Ahmadu Bello University, Nigeria

A. M. S. Tekanyi
Electrical and Computer Engineering Department, Ahmadu Bello University, Nigeria

S. M. Sani
Electrical and Computer Engineering Department, Ahmadu Bello University, Nigeria

ABSTRACT
There are scenarios in wireless networks where a fully connected path between nodes for communication through a network is not the case and yet nodes still need to communicate freely. Despite concerted efforts to resolve this problem of unconnected wireless nodes trying to relay crucial information, network users still experience significant communication challenges owing to failures or non-existence of critical infrastructural links between nodes and their security challenges. Node cooperation technique was developed and incorporated into the security aided and groups encounter PRoPHET routing protocol with cooperative behavior modelled for three nodes as shown in the cooperative behavior equation. This is in order to improve its security to ensure availability and to resist malicious dropping in OpptNets where a node may refuse to act as a relay and only settle for sending and receiving its own data or information, thus, causing considerable delay degradation in the network. Results demonstrated that, the node cooperation improved the security aided and group encounter PRoPHET routing protocol as it improved the delivery probability by 25.7%, reduced the latency by 13.10%, improved the hop count by 62.9%, and improved the buffer time by 55.5% at the end of the simulation time when compared with the delivery probability, latency, hop count and buffer time of the security aided and group encounter PRoPHET routing protocol without node cooperation.

Keywords
PRoPHET routing protocol, node cooperation, post disaster communication network

1. INTRODUCTION
The opportunistic network, also called any path routing, is characterized as a necessary evolution of traditional mobile ad-hoc network with providing wireless network properties. Opportunistic networks consist of both fixed and human-carried mobile devices (nodes) that communicate with each other with or without any infrastructure [1]. [2] During data transmission, OppNets are connected through user devices as they move, thus completing message transmission. However, this transmission method is accompanied by the security problem of uncertainty during movements. Any large-scale disasters like flood and cyclone have severe impact on communication infrastructure. Services like cell phone/internet connectivity immediately become non-functional in emergencies due to the failure of the supporting infrastructure through both system damage and system overuse [6]. Therefore, the possibility of information exchange using normal communication infrastructure is almost ruled out. According to the World Disasters Report, (2013), when disaster strikes, access to information is as important as access to food and water [7]. As identified by project RESCUE, any crisis response activity consists of several interrelated phases each of which requires appropriate situational information for its execution [8]. This acute need for information exchange demands setting up of a temporary post-disaster communication network until the normal communication infrastructure is operational again. Therefore, PRoPHET [9] one of the benchmark routing protocols for DTN, fits well for such encounter-based forwarding as it uses the history of previous encounters with other nodes, as well as the transitive properties of the network for bundle forwarding over the network [9]. However, some nodes in the opportunistic network may not be willing to participate in the routing process at all times [11]. Thus, a node may be selfish towards another node, for various reasons, for example, it might be low on resources such as battery life, memory or lack of interest in helping nodes outside its own group. In the work of [12] proposed a Trust-based Security Protocol (TSP) to mitigate black hole attacks in opportunistic networks (OpptNets) that used PRoPHET as the underling routing protocol. Trust was calculated by the destination node and distributed to each node according to its hop number in the message, Trust was distributed among other pears that had participated in the delivery process, a higher trusted node does not guarantee higher delivery probability. [13] Designed and implemented a trust management protocol for Delay Tolerant Networks (DTNs) and applied it to secure routing to demonstrate its utility. Their protocol outperformed SReD and PRoPHET, and approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead, the privacy of the information itself which may be sensitive to users was not considered.

In [3], they proposed an authentication mechanism with privacy protection for opportunistic networks. The proposed mechanism finished the authentication with less data, and provided anonymity and user privacy in the network. In their network environment, malicious attackers can tap and collect data, such as messages transmitted between devices and the super node during authentication processes.

[4] presented a security aided and group encounter based PRoPHET routing protocol that disseminated situational messages and avoided malicious nodes in the network. The trust that ensures the magnitude of cooperation in the delivery of message in the network was not considered. Therefore, we

in this paper integrate a cooperative component with their PRoPHET in other to resist the Sybil nodes more effectively.

The rest of the paper is organized as: Section 2 describes security threats and requirements in opportunistic network. Section 3 describes the methodology adopted. Section 4 presents the results obtained. Section 5 concludes the research.

2. LITERATURE REVIEW

2.1 Security Threats And Requirements In Opportunistic Networks

Opportunistic networks inherit many characteristics of DTNs and MANETs including vulnerabilities [9] but suffer from more security threats which are listed as follows:

1. *Identity Spoofing:* A malicious node may misrepresent itself by claiming to be someone else. This could be used to steal messages that are meant for a particular node.
2. *Black Hole Attack:* Malicious node acting as a black hole sets its delivery predictabilities for all destinations to a value close to or equals to 1, requests all messages from nodes it meets, and forwards none of them. A node encountering such a malicious node tries to forward all its bundles to the malicious node, creating the belief that the bundle has been very favorably forwarded.
3. *Bundle Store Overflow:* A malicious node may generate a large number of fake messages for a particular destination and fill up the buffer of a target node at the expense of other legitimate messages.

2.2. Post Disaster Relief Operation

After a large scale natural disaster, victims normally take shelter in nearby safe areas like school buildings, temporary tents in some highland areas and other risk free zones. Several disaster response agencies set up relief camps in and around the disaster affected area and mobilize manpower (volunteers) and resources to those camps in order to carry out relief operations. Each camp has a dedicated number of volunteers who provide a specific type of service relevant to the camp. For example, volunteers associated with Health Care Relief Camps will provide medical aid, whereas those associated with Logistic Relief Camps will provide relief materials like foodstuff, clothes, blankets, tents, etc. to the victims in each shelter. A command and control station is established away from the disaster affected area to organize resource distribution and coordinated relief work in the different relief camps. This leads to a coordinated and collaborated effort towards disaster rescue, response, relief, and rehabilitation.

2.3. PRoPHET for Group Encounter Routing

Situational messages are categorized according to their content and hence pertain to any one of the groups working in the disaster area. Such categorized messages need to be forwarded to their respective group relief camps for necessary action. PRoPHET depends on the following three important equations formulated as equations, (1) through equation (3) to update the delivery probability values [15]. The detail formulation of each of these equations is explained as follows:

The protocol relies on the delivery predictability metric, $P \in [0,1]$, that should reflect the probability of encountering a certain node. That metric should be used to support the decision of whether or not to forward a message to a certain node. Whenever a node is encountered, the metric should be updated according to (2), where $\mathrm{P}(A,B)$ is the delivery predictability node *A* has for node *B* and *Pinit* $\in$[0, 1] is an initialization constant according to [15], [14] . This ensures that nodes that are often encountered have high delivery predictability and the relationship of these probabilities [14] is given as:

$$P(A,B) = P(A,B)_{old} + \left(1 - P(A,B)_{old} \times Pinit\right) \quad 1$$

Where

$\mathrm{P}(A,B)$ is delivery predictability node *A* has for node *B*

Pinit $\in$[0, 1] is an initialization constant

If a pair of nodes do not encounter each other for a while, they are less likely to be good forwarders of messages to each other, thus the delivery predictability values must age [18], and is reduced in the process. The aging equation is shown in (2).. The time unit used can differ and should be defined based on the application and the expected delay in the targeted network with the aging equation [14] as:

$$P(A,B) = P(A,B)_{old} \times \gamma^{k} \quad 2$$

Where

$\gamma \in [0, 1]$ is the aging constant

k is the number of time units that have elapsed since the last time the metric was aged.

The delivery predictability also has a transitive property, that is based on the observation that if node A frequently encounters node B and node B frequently encounters node C, then node C probably is a good node to forward messages destined for node A. Equation (3) shows how this transitivity affects the delivery predictability, the equation [16] is as:

$$P(A,C) = P(AQ,C)_{old} + \left(1 - P(A,C)_{old}\right) \times P(A,B) \times P(B,C) \times \beta \quad 3$$

Where

$\beta \in [0, 1]$ is a scaling constant that decides how large an impact the transitivity should have on the delivery predictability

Apparently, in PRoPHET, a malicious node that arbitrarily claims delivery probability will be able to intercept data from other nodes and then it either drops or arbitrarily forwards them, which will detrimentally degrade the network performance.

In a typical disaster relief environment, volunteers belonging to a particular group periodically visit their corresponding relief camp for collecting resources, etc. Therefore, they can be considered as the most suitable forwarders of messages destined to that particular camp [5]. Now, due to group mobility pattern or interdependence among the groups, a volunteer belonging to a particular group encounters volunteers of its own group or some specific groups more frequently than volunteers of other groups. Therefore, it is sensible to judiciously exploit this encounter pattern for forwarding categorized situational messages to their respective destinations. PRoPHET fits well for such encounter history based forwarding as it uses the history of previous encounters with other nodes as well as the transitive properties of the network for bundle forwarding over the network [16], [10].

2.4 Node Cooperation in Opportunistic Network

In OppNets, the cooperation of nodes can be considered as the nodes probability either to drop a message copy upon its reception or to forward the message to its encountering node. The main requirement of OpptNets is that the participating nodes should be unselfish, since communication is performed with the help of other nodes. However, this might not always be the case, since selfish nodes might decide that they do not want to help others. Such nodes should be detected and not allowed to participate in the dissemination process. This way, their messages will not be delivered, so they will be forced to become unselfish if they want a good networking experience. Cooperative behavior of nodes will largely affect the performance of OppNets, For example, lack of node cooperation, where a node may refuse to act as a relay and only settle for sending and receiving its own data, causes considerable delay degradation in the networks. To deal with this issue, the general method is to enable trust across communicating entities. The establishment of trust can evaluate nodes trust level and resist the Sybil nodes more effectively in OppNets. It further helps in identifying the malicious behavior of nodes in the network. A malicious behavior leads to a considerable delay in the message delivery or no delivery at all. Cooperation and trust between nodes in the network saves them from malicious attacks. The trust of a node is the basic value that symbolizes the magnitude of its social responsibility in the network, which include helping groups of nodes in message delivery, saving these nodes from malicious attacks, timely delivery of messages.

3. METHODOLOGY

The methodology adopted in this research is as follows:

(1) Modeling the opportunistic network using the PRoPHET routing protocol.

(2)Incorporation of the node cooperation strategies in to the ONE simulator.

(3)Simulation using the ONE simulator.

3.1 Modelling Post Disaster based Scenario for PRoPHET Routing in Helsinki

This research assumes that messages are categorize on the basis of their relevance to a particular group. Thus, the following assumptions were considered.

1. Only four different types of nodes exist in a post disaster scenario.
2. Communication can only exist via Bluetooth with a communication range of 10m and a speed of 2Mbit/s.
3. Messages are grouped and categorised on their relevance to a particular group and are there by forwarded based to their corresponding group relief camp.

The choice of these assumptions was made in order to depict the real life scenario of a post disaster in terms of simulation as much as possible. Based on assumption 1, the nodes involved are detailed as follows:

(i) Transport Nodes (TN): They consist of vehicles (e.g., any type of vehicle capable of carrying food items) capable of generating situational messages about when water and other shelter items will be available.

(ii)Shelter Nodes (SN): The shelter node in this case could be a laptop, mobile phone or a work station which categorizes situational messages, stating the number of items (i.e., food, water, clothing, medicine, etc.) required in the shelter.

(iii)Camp Nodes (CN): This node received categorized messages from the different shelters and accesses their requirement to organize distribution of resources.

(iv)Forwarder Nodes (FN): These are nodes which moves around the disaster area and forward shelter messages to the relieve camps.

3.2. PRoPHET based Node Cooperation

Mutual behaviours between the nodes, where nodes do not only send and receive its own data, but participate in shearing information from others were modelled in this research. In this research, specifically, cooperative behaviour is modelled for three nodes (shelter node, camp node and forwarded node) out of the four nodes considered for the post disaster scenario. This is because, the fourth (transport node) only participate at the time of need, thus does not have constant influence on the behaviour of the network. Assuming a node NC, is sending a message through the network to another node, let's say FN. The node cooperation technique is implemented as follows:

$$DN = \begin{cases} (CN, SN) & if\ CN\ \&\ SN \le FN \\ (CN, FN) & if\ CN\ \&\ FN \le SN \\ (SN, FN) & if\ SN\ \&\ FN \le CN \\ 0 & if \quad otherwise \end{cases} \qquad (4)$$

Where

DN is the final destination node

CN in this case is the camp node

SN is the shelter node

FN is the forwarder node.

The setting subprogram for the node cooperation is given as follows:

```
package routing;
publicclass nodeCooporation {
## Scenario settings
Scenario.name = NODE COOPORATION POST DISASTER
Scenario.simulateConnections = true
Scenario.updateInterval = 0.1
# 43200s == 12h
Scenario.endTime = 10000000
Scenario.endTime = 43200
# "Bluetooth"interfacefor all nodes
btInterface.type = SimpleBroadcastInterface
# Transmit speed of 2 Mbps = 250kBps
btInterface.transmitSpeed = 250k
btInterface.transmitRange = 10
highspeedInterface.type = SimpleBroadcastInterface
highspeedInterface.transmitSpeed = 10M
highspeedInterface.transmitRange = 10
```

4. RESULT AND DISCUSSIONS

The results obtained from the application of the node cooperation strategy into the security aided and group encounter PRoPHET routing protocol on the Helsinki simulation area are shown in Tables 1 and 2, where DP represents delivery probability. Table 1 shows the result obtained for the security aided and group encounter PRoPHET routing protocol without node cooperation, while Table 2 shows the result for the security aided and group encounter PRoPHET routing protocol with node cooperation.

Table 2: Detail Result Obtained for Helsinki with node cooperation

SIM	TIME SEC	DP	Latency	Buffer time	Hop count
4000	119.70	0.2746	1925.3824	1925.3824	2.4706
8000	108.23	0.3854	2831.0300	2364.4310	2.5125
12000	238.14	0.4213	3588.8757	2795.1711	2.4412
16000	109.79	0.4146	4085.4073	2962.0377	2.4463
20000		0.4095	4273.5032	3029.6997	2.5023
24000	117.70	0.4279	4532.7804	2996.9269	2.5942
28000	114.23	0.4270	4799.5287	3020.8477	2.5981
32000	102.61	0.4500	5104.6622	3024.1300	2.5944
36000		0.4481	5245.6825	3030.3842	2.5786
40000	54.53	0.4568	5272.9118	3032.2307	2.5892
44000	122.34	0.4518	5396.9921	3067.2979	2.5970

From the Helsinki model SIM T of 44,000 in Table 2 when compared with that without node cooperation in Table 1, it was observed that the delivery probability and the buffer time were improved by 25.7% and 55.5 %, respectively and also the latency and hop count were reduced by 13.10% and 62.9%, respectively. The graphical representation of the improved security aided and group encounter PRoPHET routing protocol with node cooperation as compared with that without node cooperation is shown in Figures 1. Figure 1a shows the variation of the delivery probability with time, Figure 1b shows the variation of latency average with time, Figure 1c shows the variation of buffer time management with time while Figure 1d shows the variation of hop count with time. The plots of Figure 1 were generated using the Matlab (Matlab 2013Rb) script.

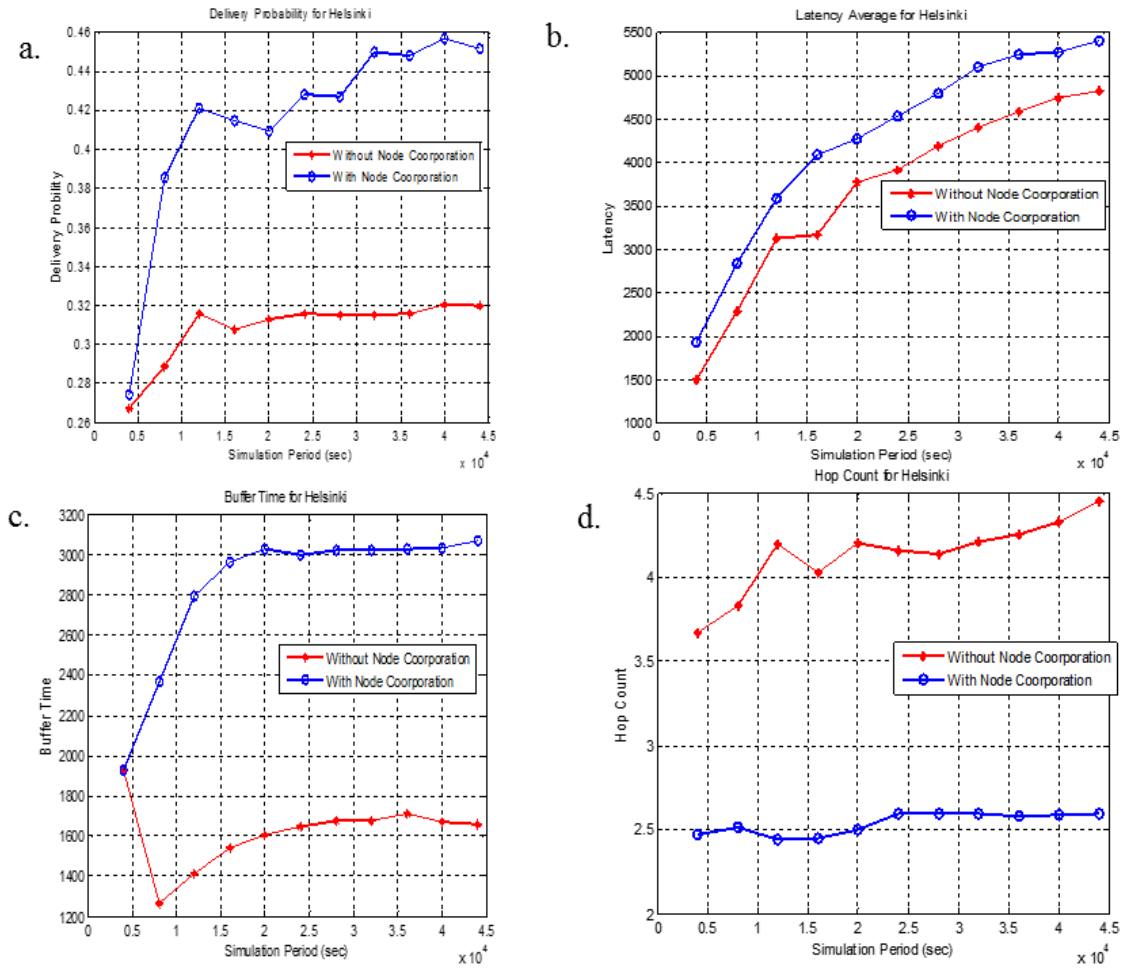

Figure1. Comparison of Security Aided and Group Encountered ProPHET RoutingProtocol of an Opportunistic Network with and without Node Cooperation

The improvement of the respective delivery probability, latency and buffer time, as well as the reduction of hop count for the Helsinki model of PRoPHET routing protocol with node cooperation are clearly illustrated in the plots of figure 1. From the response presented in Figure 1a, it shows that the delivery probability improved throughout as compared to the security aided and group encounter PRoPHET routing protocol without node cooperation. Figure 1b shows that, the security aided and group encounter PRoPHET routing protocol with node cooperation obtained a higher latency than the security aided and group encounter PRoPHET routing protocol without node cooperation. This is an indication that, the time delay between the message delivery and any possible physical attack in the network will have significant effect in the security aided and group encounter PRoPHET routing protocol without node cooperation than in the model with node cooperation. This is due to the fact that, the model with node cooperation tends to respond much better from input to desired outcome. Figure 1c shows the security aided and group encounter PRoPHET routing protocol with node cooperation has a much higher buffer time compared with the security aided and group encounter PRoPHET routing protocol without node cooperation. This is also expected since every node in the model with node cooperation has mutual behaviours by helping to distribute or pass message towards neighbouring nodes even if the message is not meant for it. In figure 1d, it can be observed that, the security aided and group encounter PRoPHET routing protocol with node cooperation has a less hop count as compared with the model without node cooperation. This is also expected since store and forward and other latencies are incurred through each hop, a large number of hops between source and destination implies lower real-time performance.

5. CONCLUSION

This work presents a security aided and group encounter PRoPHET routing protocol with node cooperation. The results showed an improvement in the security aided and group encounter PRoPHET routing protocol because, it improved the delivery probability by 25.7%, reduced the latency by 13.10%, improved the buffer time by 55.5 % and reduced the hop count by 62.9% as compared to the security aided aided and group encounter PRoPHET routing protocol without node cooperation on the bench mark Helsinki simulation area.

The vehicular mobility model can be used to evaluate the security performance of the security aided and groups encounter PRoPHET routing protocol. Also, other techniques like incentives can be integrated in to the operation of opportunistic networks to enhance node cooperation.

6. REFERENCES

[1] Papaj, J., Dobos, L. u., & Cizmár, A. (2012). Opportunistic Networks and Security. Journal of Electrical and Electronics Engineering, 5(1), 163.

[2] Huang, C.-M., Lan, K.-c., & Tsai, C.-Z. (2008). A survey of opportunistic networks. Paper presented at the Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on Advanced Information Networking. 1672-1677

[3] Guo, M.-H., Liaw, H.-T., Chiu, M.-Y., & Tsai, L.-P. (2015). Authenticating with privacy protection in opportunistic networks. Paper presented at the Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), 2015 11th International Conference on. 375-380

[4] Wu, Y., Zhao, Y., Riguidel, M., Wang, G., & Yi, P. (2015). Security and trust management in opportunistic networks: a survey. Security and Communication Networks, 8(9), 1812-1827.

[5] Basu, S., Bhattacharjee, S., Roy, S., & Bandyopadhyay, S. (2015). SAGE-PRoPHET: A Security Aided and Group Encounter based PRoPHET Routing Protocol for Dissemination of Post Disaster Situational Data. Paper presented at the Proceedings of the 2015 International Conference on Distributed Computing and Networking. 10-20

[6] Luo, H., Kravets, R., & Abdelzaher, T. (2006). The-day-after networks: A first-response edge-network architecture for disaster relief. NSF NeTS FIND Initiative, http://www. nets-find. net/Funded/DayAfterNet. php.

[7] Vinck, P. (2013). World disasters report: Focus on technology and the future of humanitarian action: International Federation of Red Cross and Red Crescent Societies.

[8] Mehrotra, S., Butts, C., Kalashnikov, D., Venkatasubramanian, N., Rao, R. R., Chockalingam, G., . . .Huyck, C. (2004). Project RESCUE: challenges in responding to the unexpected. Paper presented at the Electronic Imaging 2004. 179-192

[9] Grasic, S., Davies, E., Lindgren, A., & Doria, A. (2011). The evolution of a DTN routing protocol-PRoPHETv2. Paper presented at the Proceedings of the 6th ACM workshop on Challenged networks. 27-30

[10] Verma, A., & Srivastava, D. (2012). Integrated routing protocol for opportunistic networks. arXiv preprint arXiv:1204.1658.

[11] Ciobanu, R. I., Dobre, C., Cristea, V., Pop, F., & Xhafa, F. (2015). SPRINT-SELF: Social-Based Routing and Selfish Node Detection in Opportunistic Networks. Mobile Information Systems, 2015.

[12] Gupta, S., Dhurandher, S. K., Woungang, I., Kumar, A., & Obaidat, M. S. (2013). Trust-based Security Protocol against blackhole attacks in opportunistic networks. Paper presented at the WiMob. 724-729

[13] Chen, R., Bao, F., Chang, M., & Cho, J.-H. (2014). Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Transactions on Parallel and Distributed Systems, 25(5), 1200-1210.

[14] Lindgren, A., Doria, A., & Schelén, O. (2003b). Probabilistic routing in intermittently connected networks. ACM SIGMOBILE mobile computing and communications review, 7(3), 19-20.

[15] Lindgren, A., Doria, A., & Schelén, O. (2003a). Poster: Probabilistic routing in intermittently connected networks. Paper presented at the Proceedings of The Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003). 90-100

[16] Pelusi, L., Passarella, A., & Conti, M. (2006b). Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. Communications Magazine, IEEE, 44(11), 134-141.