A Secure and Reliable Structure in Opportunistic Networks

Samaneh Rashidibajgan, Thomas Hupperich
University Münster, Germany

samaneh.rashidibajgan@wi.uni-muenster.de , thomas.hupperich@wi.uni-muenster.de

Abstract

In Opportunistic Networks (OppNets), messages are sent to nearby nodes and forwarded from a node to another from a source to destination. An OppNet is an excellent option to shape a network in sensitive environments where fundamental infrastructure is not available. In a fragile environment (e.g., man overboard), it is essential to assure the continuous attendance of people in the network (i.e., cruise ship). In such a scenario, OppNet can be used in such a way to track individuals via constructing a network of nodes (equal to the number of passengers) Base Stations (BSs), and a monitoring system. The presence of a node that indicates on the attendance of a person is announced to the monitoring system via BSs in real-time (the same scenario for the absence). Individuals can carry a wearable device as a node. Once the lack of a node is detected in the monitoring system, an alarm is produced. This paper is a case study for detecting the presence of nodes in a sensitive environment by a secure structure. AIDAprima cruise ship with the realistic dimensions is taken into consideration in simulation. The simulation is conducted in the Opportunistic Network Environment (ONE) with 40 to 160 nodes and the length step of 20. False-positive/negative rates and incorrect classified nodes are simulated to validate the performance of the structure. Besides, the sensor tags CC2650, from Texas Instrument are used to construct the OppNet in this study.

Introduction

Opportunistic networks (OppNets) (Pelusi, Passarella, & Conti, 2006) are a new emerging wireless sensor networks in which individuals carrying wearable devices or Personal Device Assistant (PDA) (e.g., cellphone, tablet, laptop, etc.) shape the network (Conti, Giordano, May, & Passarella, 2010). In OppNets, nodes forward messages to the nearby neighbor nodes in wireless (e.g., Bluetooth, Wifi, or 4G). These networks are suggested to be used in the environments those without fundamental infrastructures. The main application areas for OppNets are search and rescue operations (Huang, Amjad, & Mishra, 2005), (Ochoa & Santos, 2015), (Anjum, Noor, & Anisi, 2015), (Reina, et al.), military communication (Jia, Chen, & Zhao, 2017), animal tracking (Juang, et al., 2002), (Ayele, Meratnia, & Havinga, 2018), and disasters (MartiN-Campillo, Crowcroft, Yoneki, & Marti, 2013) , (Hossmann, Legendre, Carta, Gunningberg, & Rohner, 2011).

In OppNet, the carry and forward method is used (Erramilli & Crovella, 2008). Nodes exchange their messages with the nodes in the range, save them in the buffer, and forward to the next available neighbors. OppNets are a kind of Delay Tolerant Networks (DTN) (Fall, 2003), but the delay of messages depends on the density of the network. The mobility of nodes is a crucial parameter to be considered. Basically, the delay is reduced when the density of nodes is increased in such networks. This fundamental feature of the OppNet can be used to track nodes (individuals) in a sensitive environment.

Every year, some people are disappearing on cruise ships due to falling in the water (man-overboard), and not the passengers nor crew notice it. There is a number of blind spots and area in the ocean which Satellite and GPS do not work as well. However, the available devices and facilities in the market are expensive and not affordable nor usable for a large number of people on a cruise ship.

As earlier was mentioned, OppNet does not need a fundamental infrastructure (MartiN-Campillo, Crowcroft, Yoneki, & Marti, 2013) and can be implemented even via small and wearable sensor tags. When there is a large density of nodes, OppNets have a short delay. As a result, OppNets can be used to shape a network and check the availability of nodes in a sensitive environment. Everyone can carry a sensor tag, and the presence of sensor tags is checked frequently. As soon as a node is disconnected from the network, an alarm can be generated.

It is essential to provide a safe environment for individuals; however, to respect network participant privacy, network security and privacy must be addressed in OppNet to make the network acceptable for individuals. People do not like to be tracked, and announce the locations or activities. In this paper, we aim at proposing a reliable structure for checking the presence of nodes in the environment. In addition, we provide identity and location privacy and anonymity for nodes. Nodes presence are checked without knowledge about their exact position or learning about the topology of the network.

The rest of this paper is organized as follows: A brief literature review is provided in Literature Review Section. The proposed secure structure and its details are described in section Proposed Structure. Simulation, results and discussions are provided in related sections, and the paper is concluded in section Conclusion.

Literature review

Providing security and privacy for nodes has been a common concern in OppNets studies. Some algorithms are proposed in the literature to address this issue. We briefly discuss the concerns, solutions, advantaged, and disadvantages.

Kate and et al. (Kate, Zaverucha, & Hengartner, 2007) proposed hierarchical identity-based cryptography to provide anonymity and security for DTNs. In this research, the user's identity was combined with the user's geographical identifiers to make it more unique. This paper assumed that DTN gateways are aware of nodes' identities, so gateways need to have knowledge about the network to route the messages.

Privacy-Enhanced Opportunistic Networking (EPON) is introduced in (Le, Vakde, & Wright, 2009). PEON proposed to put nodes in some groups, and each group shares a similar public key. Then the source can select a series of intermediate nodes and messages will receive to all members of a group. The aim of this algorithm is to hide the relationship between the source and the destination. Also, the messages are encrypted in layers, for this purpose, nodes should have knowledge about at least one hop before and after.

Jasen and et al. introduced a Threshold Pivot Scheme (TPS) in (Jansen & Beverly, 2010), and the algorithm covered the node's anonymity and their physical location privacy. In this research, nodes divided into some groups, and all member of each group has a set of public and private keys. Shamir algorithm is used in this paper to share a secret between nodes to divide messages. Messages are encrypted with the receiver's public key, and all nodes in the receiver group can decrypt it. This algorithm needs a third party for sharing keys.

A fully distributed and collaborative k-anonymity protocol (LPAF) is introduced in (Zakhary, Radenkovic, & Benslimane, 2013). In this algorithm, all trusted Friends shape a group, and these groups are based on the social activity of nodes. Then, each message is forwarded to k hops in a similar social group in order to anonymize the location of the sender.

Avatar algorithm is introduced in (Du, Zhu, Li, Ota, & Dong, 2013). Each node has some virtual nodes that shape the virtual mix zone. Each node has a footprint signature and signs its virtual nodes with this signature. Nodes change the pseudonym for themselves and their virtual nodes frequently. In order to avoid the selfish behavior of nodes, a multi-unit discriminatory auction game is used in this algorithm.

Multi-Hop location protection (MHLPP) (Huang, Ying, & Nayak, 2018) proposed to use obfuscation path to anonymize nodes location in OppNet. TMHLPP suggested hiding the sender information in its Friends information. The last Friend in a group of Friends records the sender's information to give back the answer. This paper assumed that some nodes know each other, and can shape friendship groups.

Privacy-preserving history-based (PPHB) routing algorithm is proposed to provide anonymity for nodes and privacy for nodes identity and location (Rashidibajgan & Doss, 2019). Each node calculates a NumID and a polynomial based on its ID in the network, while the NumID has to be the root of the polynomial. Then, nods multiply their polynomial to the most frequently visited nodes. Each node will check that the receiver NumID is its polynomial root or not, to decide to carry a message for a receiver or not. If it will be the root, it means that the node will visit the destination or can be a suitable candidate for carrying it.

Most of the discussed algorithms need previous knowledge about the network for forwarding messages. Furthermore, none of the algorithms introduced here was implemented in a real environment. Most of them are more complicated, and it is not possible to implement them on wearable devices. The aim of this paper is to propose a secure structure implemented in wearable sensor tags.

In this paper, a secure and reliable OppNet is proposed and implemented in which nodes can inform their presence via each other. Sensor tags CC2650 from Texas Instruments are used to shape this network in a concrete scenario. Individuals can carry these tags, and they can move in a limited environment. When a node leaves the network, its connection to other nodes is lost, then an alarm is produced for the rescue process.

The main contributions of this paper are as follows. The proposed structure:

- Introduces a secure structure for checking the presence of nodes in a sensitive environment.
- Provides location and identity privacy for nodes in the network.
- Provides anonymity for nodes in the network.
- Proposes a secure and applicable structure with low computation complexity in wearable devices.

Proposed Structure

We propose a structure with three major components: wrist-worn nodes, BSs, and a monitoring system. Each sensor tag (node) is represented with a prime number as its identification (Node_{ID}). Each node announces its attendance in which propagates through intermediate nodes to BS -- if not directly in the range of BS. Consequently, the collected information which indicates the status of nodes is forwarded to the monitoring system. The monitoring system analyzes the collected data to find out which nodes are present in the network. If a node(s) is missing, an alarm signal can be produced.

Bluetooth Low Energy (BLE) is considered as the communication interface for nodes in this paper. In general, BLE works in two modes: broadcasting mode and connection mode. In broadcasting mode, packets are broadcasting to all devices, and each device in the listing range can receive it. In connection mode, nodes should connect to each other to forward packets, and only the two paired devices can send or receive packets. In the proposed algorithm, only the broadcasting mode of BLE is used. We use the broadcasting mode because it is faster to announce the presence, and all sensor tags in the range can listen and receive the message. In the rest of this section, the structure of the proposed algorithm is described.

Network Nodes: Broadcasting, Recognition, and ID Update

In the first step, nodes should broadcast their presence to the BSs, whether if in the range directly, or via intermediate nodes. This process should be done without knowledge about the network topology or available nodes' identity. The network contains a set of nodes (Nodes=$\{n_1, n_2, n_3 \ldots, n_{160}\}$), each node has an ID based on prime number ($\text{Nodes}_{\text{ID}} = \{7, 11, 13 \ldots, 967\}$), and a set of BS/BSs (BS= $\{BS_1, BS_2, \ldots, BS_6\}$) that are stationary nodes. Prime numbers 3 and 5 are excluded from the list of IDs. The process in the network is done as follows:

- When each node powers on and is connected to the network, it attempts to find another node in Nodes set, if is in its communication range. This recognition is completed without knowledge about the ID or name of other nodes. In our implementation, nodes are set in hardware to connect only to the sensor tags belong to the OppNet. If a node recognizes another node in its communication range (a neighbor), it will multiply its ID to the neighbor's ID. For example, when the second node (n_{2ID}=11) recognizes the first node (n_{1ID}=7), it will update its ID to $n_{2\text{NewID1}} = 7 \times 11$ these are random prime number, and can be any other combinations.
$$\text{Node}_{\text{NewID}} = \text{Node}_{\text{ID}} \times \text{neighbor}_{\text{ID}} \qquad (1)$$
- Node updates its ID based on the NewID.
- This process will be repeated based on the nodes' updated ID. For example, when the third node (n_{3ID} = 13) recognizes the second node (n_{2ID} = 77) in its range, it will update its ID to n_{3ID}=1001.
- In the networks with a wide range of nodes, each node has an array, and when the Node_{ID} was greater than the Node_{ID} data type, the neighbors' ID will be saved in this array.
- Each node reset itself every 5 minutes to find other available neighbors, and the process is repeated.

Base Stations and Network Monitoring

A BS listens to the network in its range of coverage to receive broadcast nodes' IDs. The received IDs are sent to the monitoring system to analyze and extract the IDs embedded in each, which results in the detection of the attended nodes in $\mathrm{Nodes_{ID}}$ set. Each received ID is divided into all nodes ID, and if the remainder is zero, it means the related node is present in the network. So, for each $\mathrm{Node_{ID}}$:

$$\mathrm{Result} = \mathrm{Node_{ID}}\%\mathrm{ID_x} \qquad (2)$$
$$\mathrm{x} \in \mathrm{Nodes},\ \mathrm{ID_x} \in \mathrm{Nodes_{ID}}$$
$$\text{If Result} = 0 \ \rightarrow \text{node x is present in the network}$$

This procedure is done for all nodes in the network every 5 minutes, and present nodes are recorded in a table. Then the present nodes are compared with Nodes, and lost nodes are recognized.

The proposed algorithm provides the following security benefits for the network:

- Network zero-knowledge: nodes can broadcast their availability without knowledge about their neighbors or the topology of the network.
- Nodes privacy: Each node updates its ID based on neighbors, and the node's ID is dynamic. Nobody can recognize the real location or ID of neighbor nodes in the network.
- Nodes anonymity: In the proposed structure, nodes remain anonymous for other nodes in the network. The monitoring system can find out the presence of nodes without knowledge about the exact position of nodes.

Furthermore, the broadcasting mode of the BLE is used in this approach, so the proposed algorithm is so fast. It does not suffer to analyze the packets, and all nodes in the range can receive the broadcasting ID.

Simulation

A BS listens to the network in its range of coverage to receive broadcast nodes' IDs. This structure has been tested for six nodes. However, an experimental result with the scale of the cruise ship is not achievable at the moment. Therefore, besides experimental results for the small scale, including six nodes, we have simulated the network for the large and realistic network. The simulation is conducted in the Opportunistic Network Environment (ONE) (Keränen, Ott, & Kärkkäinen, 2009). The produced results in ONE are visualized in Matlab for validating the proposed structure.

We briefly describe the configuration setting of the simulation. For a better perspective and validation of the output results, the simulation area was chosen according to the realistic AIDAprima cruise ship with the dimension of 300×75 m^2. The simulation lasts for a duration of 4 hours. The coverage range of each node and the transmission speed are 23 m and 250 kbps, respectively. The network consists of 40 to 160 passengers with a step length of 20 in each execution of simulation and 1 to 6 BSs. All these items are considered as the nodes, constructing the network. The range of Passengers' maneuverability is the whole area of the so-called Cruise ship, and the direction is random. In this work, on the one hand, we are aiming at proposing a structure to detect unattended (here, man-overboard) nodes, immediately; and on the other hand, this methodology is supposed to be efficient, low-cost, easy to use, and convenient for the passengers. Therefore, to cover the whole area of the ship with the least number of BSs and the most performance, two scenarios are considered for the location of BSs and consequently, nodes' communication and network construction: 1) linear, 2) Saw tooth.

In each scenario, 11 nodes are disappeared from the network due to over closeness to the edge of the simulation area. To evaluate the performance of the structure, False Positive Rate (FPR), False Negative Rate (FNR) and the percentage of unclassified nodes (as the lost node – unattended) are calculated. To clarify:

- **False Positive Rate (FPR)**: The number of nodes in which are identified as the lost nodes, incorrectly. FRP is calculated as follow:

  $$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP+TN}} \qquad (3)$$

  Where False Positive (FP) are the present nodes in the environment but are incorrectly classified into the lost nodes, and True negative (TN) are the nodes that are lost and correctly identified as lost nodes.

- **False Negative Rate (FNR)**: The number of lost nodes that incorrectly consider as present nodes. FNR is calculated as follow:

  $$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN+TP}} \qquad (4)$$

  In equation (4), False Negative (FN) is the lost nodes that are incorrectly considered as present nodes, and True Positive (TP) is the number of nodes that are considered as the lost nodes, correctly.
- **Unclassified Loss**: It is the percentage of the attended nodes that are available in the network but classified as the lost nodes. This item is formulated as:

  $$\text{Incorrect classified lost node} = \frac{\mathrm{FP}}{\mathrm{nodes}} \qquad (5)$$

  Each scenario is conducted 6 times for 40, 60, 80, 100, 120, 140 and 160 nodes in the network with the confidential interval 95\% (CI95%). Confidential Interval 95% is shown in equations (6) and (7):

$$\mathrm{CI195\%} = \bar{\mathrm{x}} + \mathrm{z}^{*} \times \frac{\sigma}{\sqrt{\mathrm{n}}} \qquad (6), \quad \text{and} \quad \mathrm{CI295\%} = \bar{\mathrm{x}} - \mathrm{z}^{*} \times \frac{\sigma}{\sqrt{\mathrm{n}}} \qquad (7)$$

Where $\bar{x}$ is outputs' mean, $z^{*} = 1.96$, σ is outputs' standard deviation, and n=6. The simulation results in the rest of this paper are based on CI 195% from equation (6).

To validate the simulation results and test the proper functionality of the proposed algorithm, it is implemented on CC2650 sensor tags from Texas Instrument during realistic tests. These sensor tags are ultra-low power consumption, wearable, and cost-effective. CC2650 establishes BLE for communication and data transmission. We have realized that the BLE range for cc2650 is a function of several parameters (e.g., number of obstacles and the material) and is varied from 23 m to 29 m outdoor. In the simulation, the configuration range of BLE is set to the minimum; 23 m. The hardware nodes are configured in the way only to be recognized by the same nodes in the network (realistic tests).

Table 1: Base Stations environment coverage

BSs	Coverage area (%)	Uncovered area (m^2)
1	7.39	20838.94
2	14.77	19177.88
3	22.15	17516.82
4	29.53	15855.76
5	36.92	14194.70
6	44.30	12533.64

Evaluation

Scenario 1: Linear Base Stations

Figure 1 illustrates the position of BSs in a linear order. The whole surface area, which is not covered by BSs and the percentage of the area which is covered with BSs are listed in Table 1. The covered area means the area in which BSs can directly link to a node. The diameter of BS's coverage is 23 m, and the whole covered area is the sum of the area in the range BSs. The BSs are located in a similar sight, linear, and avoiding overlapping coverage. The whole area is 22500 m^2, and each BS covers an area with a total of 1661.06 m^2.

Figure 2 presents simulation results of FPR for 6 BSs under different nodes. As expected, the network with one BS has a higher FPR, and the network with 6 BSs has less FPR. Also, when the number of nodes increases, the FPR decreases.

Figure 3 presents the FNR for the different number of nodes during the first 5 minutes. When the number of nodes increases, FPR decreases, but FNR increases. The reason is that the ID of the lost nodes remains in the network for 5 minutes. After this period, it will be possible to recognize the lost nodes, if any. The parameter FNR is FNR=0 for all nodes after 10 minutes. It means that all lost nodes are identified after 10 minutes in different scenarios.

Figure 4 illustrates the percentage of nodes that are incorrectly considered as the lost nodes while they are actually attended in the network. When there is 1 BS in the network 48% to 61% of nodes, 2 BSs 32% to 37% of nodes, 3 BS 18% to 5% of nodes, 4 BSs 6% to 7% of nodes, 5 BSs 2.6% to 3.1% of nodes, and 6 BSs 1.7% to 1.9% of nodes are classified as lost nodes while they were presented in the network. By increasing the number of nodes and BSs, this fault in the classification is reduced significantly.

Figure 5 indicates the relationship between the BSs and the number of nodes with FPR. When the nodes are increasing in the network, FPR is dropped. Also, the number of BSs in the network has a meaningful impact on the performance of the network. This is expected, as the BSs are increased, the uncovered area is reduced. Thus, it is expected the number of nodes that are in the range and communicate to BS directly or through intermediate nodes without malfunction is increased.

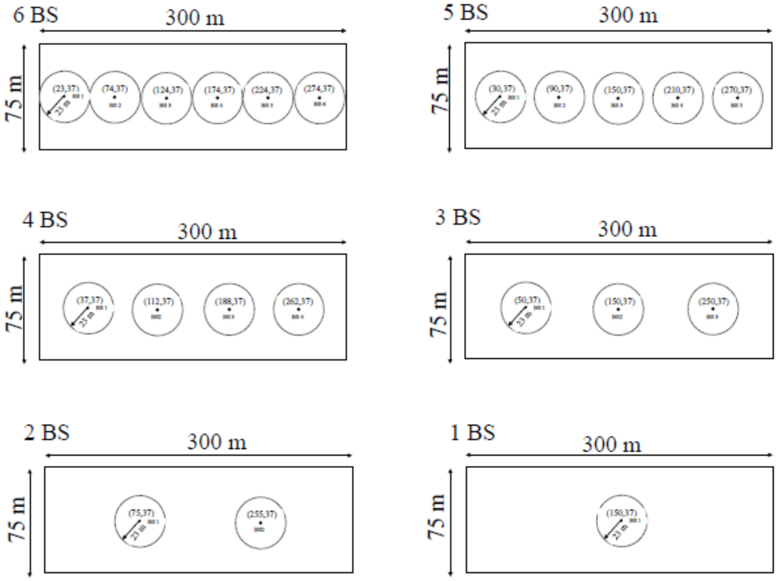

Figure 1: Position of base stations when they are shaped in a line in the simulation area

Scenario 2: Saw Tooth Base Stations

In the second scenario, we rearrange the BSs. In the first scenario, BSs are located in the straight line at the middle of surface. But in Saw tooth BSs scenario, BSs are located at top and low sides of the surface (Figure 6). Saw tooth positioning of the BSs only can be applied with BS > 3, otherwise, it does not make sense for the less number or reduces the performance in Figure 6. The covering range of none of BSs, in scenario 1 and 2 does not beyond simulation area. The ultimate range of each BS, in particular for Saw tooth scenario is limited to the edge of the area. Figure 7, Figure 8, and Figure 9 illustrate comparison of FPR, FNR, and incorrect classification for Saw tooth and linear BSs. The results show that the performance of the network is higher when BSs are located on the surface according to first scenario. In FPR, the results for BSs in are less than saw tooth, 3.99% for 4 BSs, 5.65% for 5 BSs, and 4.32% for 6 BSs. In FNR, the results for BSs in are less than saw tooth, -2.2151% for 4 BSs (in this term saw tooth was better than BSs in a line), 1.7347% for 5 BSs, and 0.04% for 6 BSs. In unclassified loss, the results for BSs in are less than saw tooth, 6.24% for 4 BSs, 7.11% for 5 BSs, and 5.20% for 6 BSs.

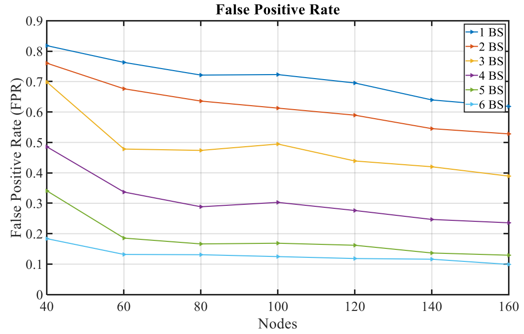

Figure 2: Comparison of false positive rate with base stations in a line

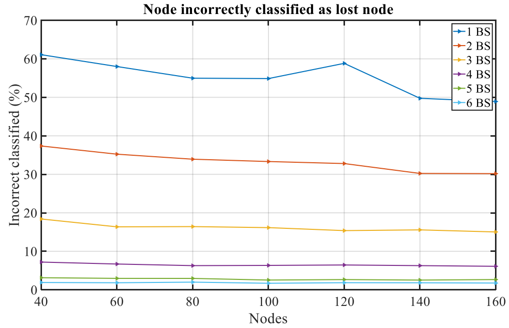

Figure 3: Comparison of unclassified nodes as lost with base stations in a line

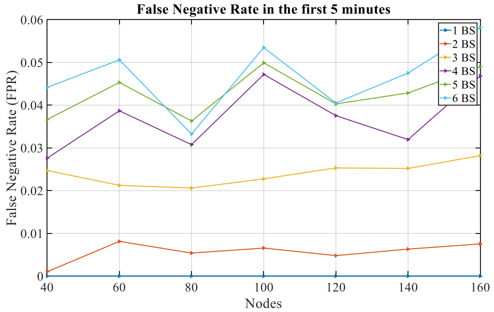

Figure 4: Comparison of false negative rate with base stations in a line

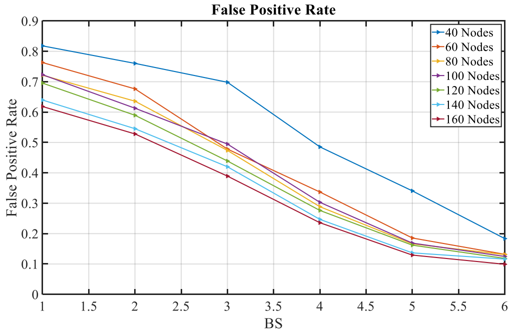

Figure 5: Comparison of false positive rate for different base stations

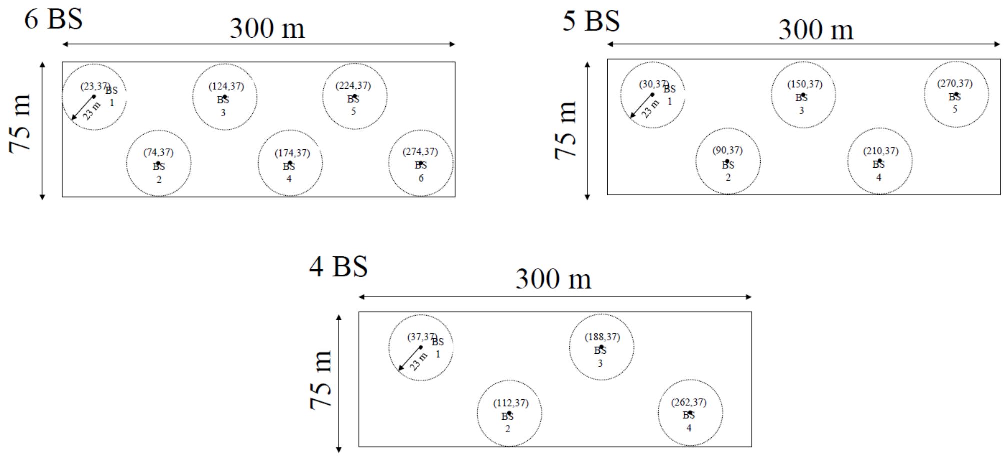

Figure 6: Position of base stations when they are shaped like saw tooth

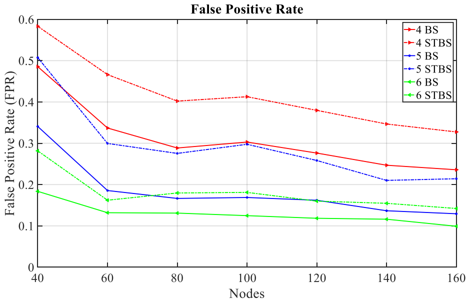

Figure 7: Comparison of FPR with BSs in a line (BS) and in Saw tooth (STBS)

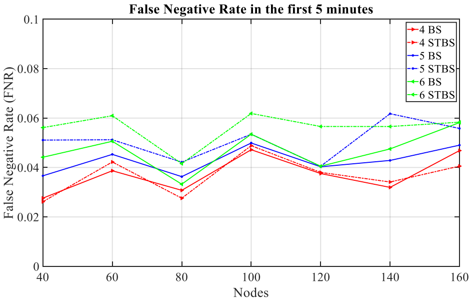

Figure 8: Comparison of FNR with BSs in a line (BS) and in Saw tooth (STBS)

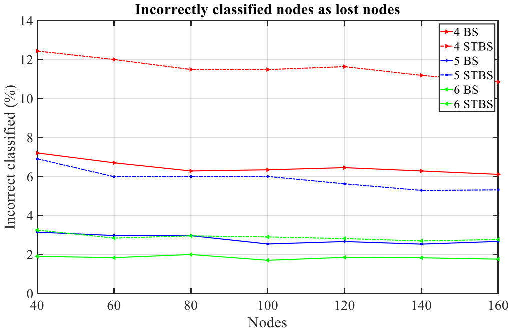

Figure 9: Comparison of unclassified nodes as lost with BSs in a line (BS) and in STBS Saw tooth (STBS)

Discussion

Tracking nodes in some sensitive environments is essential. Opportunistic networks can be a good candidate for this purpose in the environment without access to the fundamental communication environment. Since OppNets are delay tolerant networks, messages delay is a limitation. When there is a small number of nodes in the environment, FPR and misclassification are high. We have tried to show how more BSs coverage can solve this problem. The number of nodes, BSs, the range of coverage, whether by provided BSs or by nodes, and the performance of the network are in mutual relation. In OppNets, the message from the source has to reach to the destination; this can occur directly by the node to node talk, or intermediate nodes, or node to BS communication. Intermediate nodes which pass the message to the next one in the correct direction with the right decision, are playing an important role in the performance and efficiency. So that in a large network, the majority of nodes are categorized as the intermediate nodes. The availability of intermediate nodes at the end leads to the node to BS communication, and consequently, the presence of the node is detected properly. Therefore, in an OppNet, to guarantee the performance of the network, two scenarios are predicted: 1) the number of BSs is maintained low, and the number of nodes is increased. 2) The number of BSs is increased, and then the number of nodes is reduced. In this paper, we have considered both scenarios and conducted the simulation for the evaluation of the network. In the first scenario, which mostly we consider as an ideal case study, where the BS is in low number, nodes need to propagate and announce their availability through intermediate nodes. Each node, whether should directly link to a BS (low possibility due to less number of BSs) or should connect to the neighboring node. This is predictable in the large network as we simulated, to link a node at the edge of the area to the nearest BS, several intermediate nodes are involved. So, if the number of nodes, in general, is reduced; consequently, the number of intermediate nodes is decreased accordingly. This potentially puts the network in the risk of performance reduction, fault, and node disconnection. Because while a node at the edge of the area is actually available, but there is not any node around to connect and propagate to the BS. Hence, this can raise a fault by announcing the unavailability of the node in the network. The same discussion is correct for the second scenario as well. However, in this case, BSs are directly covering a higher range and potentially can link to a greater number of nodes directly. The other parameters that can significantly compensate for the lack of a smaller number of nodes and BSs are minimum covering range of the nodes and BSs.

As we showed in simulation and widely considered a number of nodes and BSs, the results are varied accordingly. However, in realistic testbed, there is a number of limitations that avoid us to play with these items freely. In the real world, each node is recognized as a person. In a cruise ship, we cannot determine the least number for boarding (of course, the maximum number is limited but is not the case here). To make it straight forward, we have limited control over the number of nodes, but here the second part of the scenario is taken into consideration. We can analyze and locate the number of BSs in different spots of the area in a way that assures adequate and full coverage. The spots identification of the BSs has been discussed widely as linear and Saw tooth scenarios. A real cruise ship is rectangular. On the one hand, in the simulation, BSs are located to not cover any area out of the edge of the ship (in reality) but edge to edge. On the other hand, to cover the random mobility of nodes, the BSs are distributed in the middle sight, which actually in comparison with lower or top sight, delivers a better output. Saw tooth is aiming at covering the edge of the area. To conclude, when the number of BSs are increased, the network performance is improved effectively. In this work, we bring two major points together to propose the tackling of man overboard issue in cruise ships, in particular. First, we propose a light, secure, and reliable structure to connect the nodes. Second, we propose using sensor tags as a wrist-worn, although with limited computation- but compatible and adequate for this purpose. We have applied our proposed structure in a wrist-worn device and utilize these sensor tags as a part of the solution into the proposed structure. As a result, according to the results and analysis of this work, OppNets are suitable for tracking nodes in crowded places or where it is possible to cover around 50% of the area with BSs.

The proposed algorithm provides nodes anonymity because nodes are defined with an ID which is dynamic and updated frequently. Also, it provides nodes identity and location privacy. Nodes' ID contain the ID of other nodes so it is not possible to recognize the exact ID or physical position of nodes. While presence of a node may receive to BS via various nodes, data integrity and confidentiality are provided. Since nodes are programed to connect to each other based on their MAC address, trust management, nodes cooperation and data access control were not considered in this research.

Conclusion

A secure and reliable structure for tracking nodes in sensitive areas based on OppNet is proposed in this paper. Each node is initially identified by a prime number in the network. During the network expansion with involving a greater number of active nodes, nodes multiply their ID to the nodes in their range and then update their ID. Thus, each node's ID is frequently update and is considered as a dynamic ID. Nodes broadcast their updated ID to the network, so each node's ID contains also the neighbors' ID if are in the communication range and connected. There are BSs in the environment that are listening to the network to receive nodes' IDs. BSs send the received IDs to the monitoring system. The IDs are analyzed to extract and recognize the information of the lost nodes in the network. To maintain the privacy and identity, each node broadcasts the neighbor's ID without knowledge about the exact location or ID of nodes. Therefore, nodes remain anonymous in the network and their privacy is protected.

The proposed algorithm is implemented on CC2650 sensor tags and simulated in ONE under two scenarios of linear and Saw tooth. The results of simulation show that when BSs are placed in the straight sight, the network delivers a better performance rather than Saw tooth. Also, when the number of nodes increases, the performance of the network is improved. The best results are related to when there are 6 BSs in the environment and more area is covered and in the range of BSs; the FPR is around 0.1, and around 1.7% of nodes are classified incorrectly.

References

Anjum, S., Noor, R., & Anisi, M. (2015). Survey on MANET based communication scenarios for search and rescue operations. *5th International Conference on IT Convergence and Security (ICITCS)*, 1--5.

Ayele, E., Meratnia, N., & Havinga, P. (2018). Towards a new opportunistic IoT network architecture for wildlife monitoring system. *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1--5.

Conti, M., Giordano, S., May, M., & Passarella, A. (2010). From opportunistic networks to opportunistic computing. *IEEE Communications Magazine*, 126--139.

Du, S., Zhu, H., Li, X., Ota, K., & Dong, M. (2013). MixZone in motion: achieving dynamically cooperative location privacy protection in delay-tolerant networks. *IEEE Transactions on Vehicular Technology*, 4565--4575.

Erramilli, V., & Crovella, M. (2008). Forwarding in opportunistic networks with resource constraints. *Proceedings of the third ACM workshop on Challenged networks*, 41--48.

Fall, K. (2003). A delay-tolerant network architecture for challenged internets. *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, 27--34.

Hossmann, T., Legendre, F., Carta, P., Gunningberg, P., & Rohner, C. (2011). Twitter in disaster mode: Opportunistic communication and distribution of sensor data in emergencies. *Proceedings of the 3rd Extreme Conference on Communication: The Amazon Expedition*.

Huang, J.-H., Amjad, S., & Mishra, S. (2005). Cenwits: a sensor-based loosely coupled search and rescue system using witnesses. *Proceedings of the 3rd international conference on Embedded networked sensor systems*, 180--191.

Huang, R., Ying, B., & Nayak, A. (2018). Protecting location privacy in opportunistic mobile social networks. *IEEE/IFIP Network Operations and Management Symposium*, 1--8.

Jansen, R., & Beverly, R. (2010). Toward anonymity in delay tolerant networks: threshold pivot scheme. *2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, 587--592.

Jia, W., Chen, Z., & Zhao, M. (2017). Effective information transmission based on socialization nodes in opportunistic networks. *Computer networks*, 297--305.

Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L., & Rubenstein, D. (2002). Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet. *ACM SIGARCH Computer Architecture News*, 96--107.

Kate, A., Zaverucha, G., & Hengartner, U. (2007). Anonymity and security in delay tolerant networks. *Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, 504--513.

Keränen, A., Ott, J., & Kärkkäinen, T. (2009). The ONE Simulator for DTN Protocol Evaluation. *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*.

Le, Z., Vakde, G., & Wright, M. (2009). PEON: privacy-enhanced opportunistic networks with applications in assistive environments. *Proceedings of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments*, 76.

MartiN-Campillo, A., Crowcroft, J., Yoneki, E., & Marti, R. (2013). Evaluating opportunistic networks in disaster scenarios. *Journal of Network and computer applications*, 870--880.

Ochoa, S., & Santos, R. (2015). Human-centric wireless sensor networks to improve information availability during urban search and rescue activities. *Information Fusion*, 71--84.

Pelusi, L., Passarella, A., & Conti, M. (2006). Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. *IEEE communications Magazine*, 134--141.

Rashidibajgan, S., & Doss, R. (2019). Privacy-preserving history-based routing in Opportunistic Networks. *Computers & Security*, 244--255.

Reina, D., Askalani, M., Toral, S., Barrero, F., Asimakopoulou, E., & Bessis, N. (n.d.). A survey on multihop ad hoc networks for disaster response scenarios. *International Journal of Distributed Sensor Networks*, 2015.

Zakhary, S., Radenkovic, M., & Benslimane, A. (2013). Efficient location privacy-aware forwarding in opportunistic mobile networks. *IEEE Transactions on Vehicular Technology*, 893--906.