Resilience and Security of Opportunistic Communications for Emergency Evacuation

Gokce Gorbil
Imperial College London
Dept. of Electrical and Electronic Eng.
Intelligent Systems and Networks Group
Exhibition Road, South Kensington
SW7 2AZ, London, United Kingdom
g.gorbil@imperial.ac.uk

Erol Gelenbe
Imperial College London
Dept. of Electrical and Electronic Eng.
Intelligent Systems and Networks Group
Exhibition Road, South Kensington
SW7 2AZ, London, United Kingdom
e.gelenbe@imperial.ac.uk

ABSTRACT

We describe an autonomous emergency support system (ESS) based on opportunistic communications (oppcomms) to support navigation and evacuation of civilians in built environments. In our proposed system, civilians are equipped with low-cost human wearable devices that employ oppcomms to exchange packets at close range of a few meters with limited or no infrastructure. This paper investigates the resilience and performance of oppcomms in the presence of network attacks. We assume that a portion of nodes in the network have been compromised and misbehave, which adversely affects communications and evacuation. We evaluate the effect of three types of node misbehaviour and propose a defense mechanism against the most serious among these. The defense mechanism combines identity-based cryptography with collaborative malicious packet detection and blacklisting of detected attackers. Results from simulation experiments conducted on a specialized emergency simulator show the impact of misbehaviour on evacuation and communication performance and the improvement offered by the defense mechanism.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*store and forward networks, wireless communication*; C.2.0 [**Computer-Communication Networks**]: General—*security and protection*; I.6.3 [**Simulation and Modeling**]: Applications; H.4.3 [**Information Systems Applications**]: Communications Applications

General Terms

Security, Performance, Experimentation

PM2HW2N'12, October 21–22, 2012, Paphos, Cyprus.

Keywords

Opportunistic communication, delay tolerant network, disaster management, emergency support, building evacuation, communications security, identity-based cryptography.

1. INTRODUCTION

In urban emergencies, the safe and quick evacuation of people in the affected area is important to minimize casualties. Such evacuation is complicated due to dynamic conditions, such as a spreading hazard and moving civilians, and safe paths may rapidly change. Furthermore, people may have an incomplete and possibly incorrect view of the situation, which may lead to incorrect decisions. Difficulty of evacuation is exacerbated by the impact of the emergency on existing communication infrastructure, which may become unavailable due to failure or congestion. Thus in this paper, we describe an **autonomous emergency support system** (ESS) based on **opportunistic communications** (oppcomms) to rapidly inform and safely evacuate people in the implicated area when other means of communication have broken down. ESS uses opportunistic contacts between wireless communication devices carried by people and other fixed sensors to gather and disseminate information on current conditions. A mobile device provides step-by-step guidance to her user based on information received via oppcomms, its local view of the area and its current location.

Timely dissemination of correct information is important in the effective operation of ESS. We investigate the resilience and security of oppcomms in this emergency context and consider that some of the communication nodes have been compromised and misbehave, which adversely affects the quality and correctness of navigation services offered by ESS. We introduce our proposed system in Sec. 3. In Sec. 4, we present three types of misbehaviour and propose a simple yet effective defense mechanism against one of the more serious of these. Section 5 presents our evaluation of the effect of these misbehaviours and the performance of our proposed defense mechanism based on simulation experiments. We discuss potential shortcomings of our approach and propose future enhancements in Sec. 6.

2. RELATED WORK

Related work in civilian navigation and emergency evacuation includes work by Tseng et al. [32] who propose a

distributed navigation algorithm based on the temporally ordered routing algorithm (TORA) for mobile ad hoc networks in order to guide civilians in a building during an emergency. In [27] the work in [32] is extended to 3D indoor building environments. In [3] a distributed wireless sensor network (WSN)-based building evacuation algorithm that takes into account the expected spread of the hazard inside the building is discussed. In [25,35] congestion during evacuation is taken into account. Other work [23] presents an autonomous indoor navigation system based on mobile phones that assumes a WSN to monitor the building and receive updates on a dynamic hazard, with a centralized emergency guidance system. A WSN of immobile nodes or a similar fixed wireless network is the main component that provides navigation support in the works discussed above.

Previous work by our group [13,14] proposes a distributed evacuation system (DES) for building evacuation, where static decision nodes (DNs) with communication and processing capabilities are installed in the building and provide directions to civilians in their vicinity, either via dynamic signs or wireless communications. DNs form a fixed wireless network and calculate evacuation paths in a distributed manner based only on local information. The approach we take in ESS is significantly different both from our group's previous work regarding DES and other systems discussed above, since the ESS uses a *mobile opportunistic communication network* (oppnet) as the basis for the provisioning of navigation services. Furthermore, none of the mentioned systems has been evaluated in terms of security of communications or how attacks on the system may affect performance.

Several authors have proposed the use of oppcomms and delay tolerant networks (DTNs) [11] for emergency support and management. Bruno et al. [4] propose the use of an opportunistic network in order to "glue" together parts of the surviving communication infrastructure after a disaster. They evaluate the communication performance of two opportunistic routing protocols, epidemic routing and HiBOp, in an emergency context. Communication performance of a modified epidemic routing protocol is evaluated in [37], where oppcomms among smartphones are proposed for the dissemination of information when cellular infrastructure is unavailable due to a disaster. A similar approach is also proposed in [24], where the authors also discuss some of the security issues of DTNs in an emergency setting. Camara et al. [6] propose a hybrid DTN infrastructure consisting of fixed road side units and mobile vehicles for the dissemination of public safety messages during emergencies in outdoor urban areas. The dissemination of information on the area layout and hazard via oppcomms is considered in [36] for emergency evacuation. None of the DTN works discussed here, with the exception of [36], consider the use of oppcomms for evacuation support, and they focus on the communication performance of oppcomms without evaluating issues of security or resilience.

Our initial evaluation in [22] showed that oppcomms can successfully enable navigation services for evacuation in confined spaces. In [21], we compared the evacuation performance of DES and ESS, and observed that given enough population density, ESS can perform as well as DES and even surpass it. We looked at how spatial parameters such as sensor and communication range affect evacuation with ESS in [15] and investigated how ESS can be used as a backup system to deal with system failures in [12].

Although previous work has discussed security issues of oppnets and DTNs, to the best of our knowledge, our work presented here is the first investigation into security of oppcomms in the context of emergency navigation and evacuation. Challenges of securing DTNs are discussed in [1,26]. Seth & Keshav [29] propose a practical end-to-end security scheme for DTNs based on hierarchical identity-based cryptography. Burgess et al. [5] look at the problem of malicious users in DTNs that do not employ security mechanisms. Choo et al. [7] investigate the same problem as in [5] but consider more sophisticated attacks; their results indicate that when attackers have better knowledge of the workings of a DTN (e.g. the details of the routing protocol), they can formulate more devastating attacks. Identity spoofing is investigated in [33] in unsecured DTNs that employ quota-based multi-copy routing protocols. Their proposed defense does not detect the spoofers or prevent them from participating in oppcomms. A reputation-based trust scheme is proposed in [2] to detect malicious nodes in a DTN. However, the long time needed to build reputation in the proposed scheme, and its complexity and overhead hamper its practical application in emergencies.

3. EMERGENCY SUPPORT SYSTEM

Our proposed emergency support system (ESS) [21,22] is targeted for densely populated urban areas, and more specifically for built environments, such as buildings, campuses and shopping malls. In this discussion, we describe the ESS as deployed in a multi-floor building. ESS has a hybrid infrastructure, consisting of **fixed sensor nodes (SNs)** and **mobile communication nodes (CNs)**. SNs are battery-powered devices pre-deployed at fixed locations in the building and monitor the environment for possible hazards. Each SN has a sensing unit that senses its immediate area (e.g. for contaminants, smoke, or excessive heat) and has short range (< 5m) wireless communication capability so it can directly communicate with CNs in range. SNs have very low memory capacity and processing power, i.e. as much as necessary to perform the sensing and communication functions, and are assumed to be energy-limited, making power consumption a major consideration for SNs. Therefore, SNs are only used for environment monitoring and indoor CN localization.

Each civilian is equipped with a hand- or pocket-held device with some memory and a processing unit, capable of short-range communication (~10m indoors). CNs can be specialized devices, e.g. very small wearable computers that are given out to employees or students by their company or university, and such devices may be incorporated into existing accessories such as ID badges and cardholders. We believe such a scheme is practical given the low cost of such devices and their potential for delivering other services in addition to emergency-related services as considered in this paper. Another option is to depend on consumer products already owned by people, such as smartphones with Bluetooth connectivity. Given that infrastructure-based communications can be disrupted during the emergency, such devices should not depend solely on cellular communications or WLANs for connectivity in emergencies. Therefore, CNs form a network in an opportunistic manner as devices come into contact as a result of human mobility. If necessary, certain nodes may be placed in fixed locations, e.g. on walls, for additional coverage. Oppcomms enable the dissemination of messages in order to gather and convey emergency informa-

tion. While we consider the singular use of oppcomms in this paper, we are in no way implying that oppcomms should be prefered to other communications, such as WLANs and cellular networks, that may provide better connectivity if they are available. Thus one can think of oppcomms and the ESS described in this paper as a back-up system that becomes operational should other emergency systems fail.

Oppcomms are characterized by the "store-carry-forward" paradigm [28] where CNs carry messages in local storage on behalf of others, and then forward them to other CNs when they meet; the choice of which messages to forward to which nodes is determined by an opportunistic routing protocol. Thus the message is delivered to its destination via successive opportunistic contacts. Because the network may be disconnected for long periods of time, carrier nodes may store messages for lengths of time, and the delivery of messages to destinations is not guaranteed. The ESS design assumes that each CN will (a) store the graph representation of the building that is described below, and (b) be able to carry out the computations that the ESS needs, sense other CNs in its vicinity, and carry out short range store-and-forward packet reception and transmission for oppcomms.

In ESS, the building is represented as a graph $G(V, E)$; vertices V are locations where civilians may congregate and move, and edges E represent path segments that civilians may follow. An edge has three associated costs: physical length, hazard intensity, and effective length, which is a joint metric that combines physical length and hazard. The building graph is known for a building since its layout and edge lengths will be static and therefore it can be created once and stored for later use. Each CN stores in local memory the building graph, which is obtained and installed through a trusted source (i.e. the company intra-net).

Each SN has a unique device ID, a local clock and a location tag that corresponds to its position in the building. SNs periodically take measurements of their surroundings and a hazard is detected when a significant measurement is observed (e.g. existence of smoke, or high temperature). Each significant measurement is kept in the form of a **measurement message (MM)** in the SN and passed on to nearby CNs via single hop communication. When active, CNs produce a periodic beacon message in the form of a localization request; any SN in the vicinity that receives the beacon replies with a **localization message (LM)** that is used by the CN to position itself in the building using the location tag in the LM(s). The actual position of a CN is therefore approximated by its location on the building graph, i.e. its corresponding graph vertex. The small communication range of SNs help to reduce localization error. In order to preserve SN energy, CNs keep their localization procedure inactive until alerted by the system of an emergency.

Each received MM is converted by the CN into a network-specific **emergency message (EM)**; an EM contains the location of the SN for the corresponding MM, hazard intensity, source CN ID and observation timestamp of the SN. Each EM is then disseminated among CNs using oppcomms; each EM is a network-wide broadcast packet. The first received MM or EM is an indication of a (new) hazard, and the CN alerts its user and starts the evacuation process for that user. Since each CN has the complete building graph, it can update its local graph using the MMs and EMs and run a shortest path (SP) algorithm[1] from its current location to the nearest exit. This SP is used to provide vertex-to-vertex directions to the civilian for evacuation; as new messages are received, the SP is updated. Since effective edges lengths are used in SP calculation, the SP is a combination of the physical distance and risk of exposure to the hazard between two locations. Therefore, the "shortest" path minimizes travel distance while avoiding dangerous areas in the building. ESS employs (prioritized) epidemic routing [34] for the dissemination of EMs. Epidemic routing is a multi-copy flooding-based protocol that mimics the spread of an infectious disease within a population. We use it in ESS due to its flooding-based approach which closely matches the "one-to-all" dissemination of EMs, and its high message delivery ratio and low latency [31]. CNs employ *timestamp-priority queues* for network storage management, where messages with the earliest creation timestamps are dropped from the queue when the queue is full. Newer messages are also given priority during transmission at CN contacts.

4. SECURITY OF OPPORTUNISTIC COMMUNICATIONS

Emergency evacuation is a crucial component of emergency response and ESS can provide effective evacuation guidance in urban areas [21,22] via oppcomms when other means of communication have broken down. Opportunistic networks (oppnets) are a form of delay/disruption tolerant network (DTN) [11] and they offer a means of infrastructureless communication in the face of intermittent connectivity. As such, oppnets are quite resilient to node and link failures and other sorts of disruptions that would render more traditional networks inoperable. However, attacks on the network and misbehaviour of nodes in the oppnet can adversely affect communication performance [5,7] and evacuation outcome.

Attacks on the emergency network can be deliberate, as in the case of terrorist attacks where the perpetrators target emergency services in an effort to multiply the effectiveness of their attack. A cheap and inconspicuous method of supplementing their attack is disseminating malware which is activated during the emergency. The system is particularly susceptible to malware when popular consumer devices are used as CNs. Another interesting case is when such attackers are present in the area to observe and coordinate their attack, and maliciously participate in the emergency response process as civilians. Other attacks or selfish behaviour by the nodes may not target the emergency process directly, but may nevertheless have an adverse impact. For example, a node can selfishly receive all messages destined for itself but may otherwise fail to participate in their propagation. Other selfish behaviour may arise when a node does not comply with the rules of the MAC protocol in an effort to get an unfair share of access to the shared medium. Thus we consider that a portion of CNs have been compromised, either as a result of malware or deliberate tampering by their users. Compromised nodes misbehave in certain ways that affect communication and evacuation. We investigate the effect of three types of misbehaviour in this paper. We would like to note that this is not an exhaustive investigation into security of oppcomms for emergency support, and that it is certainly possible to construct a different set of assumptions

[1]We assume that a CN runs Dijkstra's SP algorithm to find the "shortest" evacuation path in our evaluation.

regarding the attack models. The misbehaviours considered in this paper are used as representatives of a wider range of similar misbehaviour; they are simple to implement but either hard to defend against at the network layer or have a considerable effect on evacuation outcome.

4.1 Attack Model

We assume that there are one or more misbehaving nodes, interchangeably called malicious nodes or attackers, participating in the ESS. All non-malicious (normal) nodes operate correctly. When a defense mechanism is not employed, normal nodes trust all CNs and assume that all EMs contain correct information. We assume that each malicious node knows the identities of all malicious nodes, but attackers do not use a collaborative attack strategy. We consider three types of misbehaviour: **(i) drop-all, (ii) radio frequency (RF) jamming, and (iii) false info**.

With *drop-all behaviour*, malicious nodes drop all incoming messages. With *RF jamming*, we assume that malicious nodes generate random noise on the radio channel with enough power to disrupt communications by reducing the signal-to-raise ratio. Any nodes within range of an RF jammer cannot receive messages; depending on the MAC protocol used, they may also be unable to send messages. In our evaluation, we assume that CNs are IEEE 802.15.4 compliant and therefore use CSMA-CA[2] at the MAC layer. This means that CNs in range of RF jammers will not be able to send messages due to the carrier sensing mechanism. *False info behaviour* combines drop-all behaviour with injection of incorrect packets into the network. Under false info misbehaviour, malicious nodes drop all legitimate messages, but keep and forward malicious packets. Additionally, they generate malicious messages with false information, which is a combined network- and application-layer attack. The injection of these messages affects oppcomms performance and their content misguides CNs to provide incorrect evacuation directions. The rate of malicious message generation is controlled by the message generation probability p_{msg}: a malicious node produces a malicious messages every time it changes its location with probability p_{msg}.

Each false EM can potentially contain incorrect information on any message field: source CN ID, hazard intensity, location and timestamp. Hazard intensity, location and timestamp information is normally provided by an SN. In our evaluation, we assume that malicious nodes spoof their ID and hazard intensity but use correct values for the location and timestamp (as received from SNs by MMs or LMs) when there is no defense mechanism. In this case, malicious nodes can also modify legitimate messages received from other nodes. When there is a defense mechanism, malicious nodes only spoof hazard intensity and do not modify EMs of others to avoid quick detection.

Malicious nodes ignore received malicious packets for local updates. We assume that malicious nodes start to misbehave when they are notified of an emergency. With drop-all and false info attacks, malicious nodes guide their users based on received normal EMs. With RF jamming, malicious nodes are assumed to be unable to receive EMs once the jamming is active, and therefore guide their users without updates from EMs.

[2]CSMA-CA: Carrier sense multiple access with collision avoidance

4.2 Defense Mechanism

Our evaluation (Sec. 5) shows that RF jamming and false info misbehaviours have a significant effect on evacuation outcome and communication performance. Although RF jamming is easy to detect, it is difficult to defend against it with network-layer techniques. We therefore focus on detection of and defense against false info misbehaviour. We propose a collaborative defense mechanism that combines identity-based signatures (IBS) [30] and content-based message verification to detect malicious packets and nodes. Packet dropping and collective blacklisting is employed to prevent identified attackers from participating in oppcomms. IBS is an attractive and practical solution to provide node authentication and message integrity in DTNs. It is based on identity-based cryptography (IBC) which is an asymmetric cryptosystem that uses the well-known unique identifier, such as the network address, of an entity to generate its public key. This allows any node to generate the public key of a node with a known ID. The corresponding private key is generated by the private key generator (PKG) and known only to the entity with the given ID and the PKG.

We assume that a trusted third party acts as the PKG and assures the one-to-one correspondence between a CN and its ID. We believe this to be a valid assumption since this trusted role can be fulfilled by the system that provides the area graph to the CNs. Since this set-up step is done offline, the presence of the PKG during emergency operation is not required. The uniqueness of IDs, combined with IBS, prevents node replication and Sybil attacks [9]. Notice that IBS cannot prevent insider attacks where nodes are compromised after initial set-up.

Using IBS, each EM is signed by its source CN using its private key. A receiver can then verify the integrity and authenticity of the message using the public key generated by the receiver using the source's ID. Any message that fails verification is dropped and ignored. This scheme allows detection of spoofed IDs and of EMs modified in transit by malicious nodes. However, an additional scheme is required in order to detect malicious messages with incorrect content. Therefore, CNs employ content-based message verification in addition to IBS to detect malicious packets.

Messages received from SNs and other CNs are used by each CN to verify the content of a received EM. A CN would expect each EM to contain information consistent with the nature of the hazard and previously received EMs. For example, hazard intensity would be expected to stay the same or increase at a location, unless there are emergency response teams in the area. Information inconsistent with what is already known to the CN is flagged as suspicious. If an EM contradicts with an MM, i.e. a direct observation of the hazard, then it can be concluded that the EM is definitely incorrect and its source node is malicious. A malicious packet is undeniably tied to its source node since IBS guarantees message authenticity and integrity.

If a contradiction arises between EMs, then the fact that malicious nodes generate more messages than normal nodes is used to identify the malicious message, and thus the attacker. In this case, the source that has generated more EMs is identified as an attacker. In order to control the level of evidence required before a node is identified as malicious in this manner, the node can check that the ratio of the number of EMs is higher than a certain threshold, which can be adjusted to change the level of evidence required. This

detection mechanism does not guarantee that all malicious messages or nodes will be correctly identified since nodes need some time to gather the evidence required. Detection can also produce false negatives where a normal node is mistakenly identified as malicious. We present simulation results on the performance of detection in Sec. 5. Note that although malicious nodes may try to prevent detection by decreasing the number of malicious messages they generate, e.g. by decreasing p_{msg}, our evaluations[3] have shown that using a low p_{msg} (e.g. $p_{\text{msg}} = 0.1$) is not a good strategy since while detection ratio decreases a little with decreasing p_{msg}, the effect of the attack on evacuation performance decreases much more significantly. Therefore, normal nodes are still better off when attackers generate less messages even though the defense mechanism may be able to identify less of the malicious messages.

Messages from nodes identified as malicious are ignored and dropped by normal nodes. Collective blacklisting is used to inform other CNs of detected attackers. Each CN maintains a local blacklist of IDs of nodes detected as malicious. When a new malicious node is identified by a CN, it is added to its local blacklist and a new **blacklist message (BM)** is generated that contains the proof of identification in the form of the original messages used for the identification. Inclusion of the proof allows receivers to decide for themselves whether the identification is valid and allows the detection of false BMs that may be created by malicious nodes. As with EMs, BMs are signed by their sources and disseminated among CNs via oppcomms. BMs have higher priority than EMs to allow for their quick dissemination. A BM is piggybacked on a packet bundle when there are EMs to be exchanged during a contact. Otherwise, the BM is sent on its own. BMs are used by receivers to update their blacklists. When a CN adds a new node to its blacklist, any previous messages originating from the attacker are removed from the message queue and updates resulting from these messages are revoked.

Our proposed defense mechanism expectedly adds some overhead: communication and storage overheads result from blacklists, BMs, and message signatures, whereas the signing and verification of each message and the extra steps required for content-based verification of EMs increase the computational load of CNs. Our results in the next section provide an insight into the communication and storage overheads due to the defense mechanism. Current consumer devices, e.g. smartphones, would certainly be able to handle the additional computational load, but specialized low-cost devices may struggle with the extra load. Although using simpler cryptographic methods such as symmetric cryptography is possible to decrease the computational load, they introduce other challenges which may be more difficult to address, such as key distribution, maintenance and storage. For example, if a single symmetric key shared among all nodes is used, then our proposed defense mechanism would not be able to provide authentication or integrity since malicious nodes would have access to the same key used by everyone. If different symmetric keys are used for each node, then a node needs to store the keys for all other nodes since it can potentially receive a message from anyone and it cannot contact a key server to request an unknown key under intermittent connectivity[4]. These problems are not confined to symmetric cryptosystems either as some asymmetric cryptosystems such as those based on public-key infrastructures also exhibit similar problems with intermittent connectivity. The challenges of using conventional security methods in DTNs and oppnets are discussed in more detail in [1,26,29].

[3]Not presented here due to space limitations

[4]Note that although oppcomms may provide access to a key server under intermittent connectivity, the best-effort nature of oppcomms and the long delays would render such an option undesirable. Furthermore, the key server itself may come under a DoS attack or otherwise be unavailable, e.g. due to power or network failure.

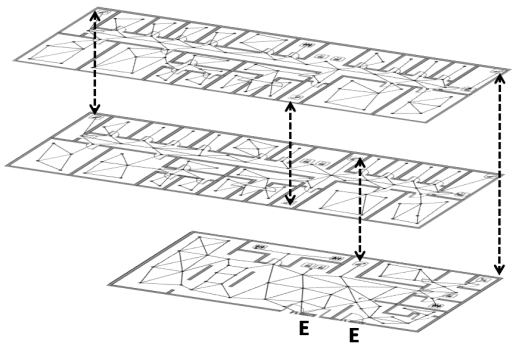


Figure 1: Building model used in our simulations.

5. EVALUATION

We have evaluated the effect of the misbehaviours described in Sec. 4 on communication and evacuation performance, and the improvement offered by our proposed defense mechanism by simulation experiments conducted with the Distributed Building Evacuation Simulator (DBES) [8] developed by our group. DBES is a multi-agent distributed simulation platform designed for the evaluation and testing of emergency systems and scenarios. We simulate evacuation of a real-life three-floor large office building, the model of which is given in Fig. 1. The bottom floor, of size 24m x 45m, contains the two exits; the upper floors are 24m x 60m. We assume a fire starts on the intersection of the two corridors on the second floor and spreads in the building following a Bernoulli trial model. The fire model and its effect on civilian health are influenced by [10]. We assume that all conventional means of digital communication have broken down in the building and that the central alarm has failed, which can be due to a central power failure. Civilians are notified of the emergency and navigated to the exits using ESS and oppcomms.

We simulate a total of 120 people in the building, initially distributed evenly and randomly among floors, i.e. 40 people per floor (pf). They follow a probabilistic mobility model until they are notified of the emergency, which simulates their movement during working hours in the building. Malicious nodes are chosen at random among all CNs. The movement speed for a civilian is 1.39 m/sec within the floors and 0.7 m/sec when traversing stairs. The simulations take physical congestion into account during human movement. Each data point is presented with its 95% confidence interval and is a mean of 50 simulation runs. Each run represents a different initial distribution of people, malicious nodes and fire spreading pattern.

We assume that in addition to the building graph and edge costs, each CN can store 100 messages (EMs and BMs). Average EM and BM sizes are 40 bytes and 100 bytes respectively without signatures. We assume that 128-bit signatures are used, which adds 16 bytes to each signed message. Maximum CN data transfer rate is 100 kbits/sec and the maximum effective CN communication range is 6m. We assume that CNs cannot communicate inter-floors, which may be due to physical factors such as floor thickness. An SN is located at each graph vertex in the building; SN data transfer rate is assumed to be 20 kbits/sec and the maximum effective SN communication range is 5m. For false info behaviour, we set $p_{\text{msg}} = 0.8$.

We first present results on the effect of misbehaving nodes on evacuation outcome. Figure 2a shows the evacuation ratio vs. number of malicious nodes. Evacuation ratio is the ratio of the number of successfully evacuated normal users to the number of all normal users. We observe that drop-all behaviour does not have a significant effect on evacuation ratio, and the effect of RF jamming is also small compared with the considerable effect of false info behaviour. The significance of the false info attack arises from its direct effect on evacuation directions provided by CNs. Due to incorrect information, CNs misguide their users, resulting in many casualties and poor evacuation performance. The defense mechanism greatly improves evacuation ratio, especially when the number of malicious nodes is low, although evacuation performance without any misbehaviour cannot be attained even with defense. This is because only some of the malicious nodes and packets can be correctly identified using the defense mechanism, as discussed later. These results also indicate that with the false info attack, even a single attacker can significantly degrade evacuation ratio, and the severity of the attack increases as the number of malicious nodes increase.

Average evacuee health is a complementary evacuation metric, which is the mean health of all successfully evacuated normal users (out of 100). Figure 2b gives average evacuee health vs. number of malicious nodes and performance similar to evacuation ratio is observed. We see that the defense mechanism improves evacuee health but the improvement is less than the improvement in evacuation ratio. Looking at these results on both evacuation ratio and evacuee health assures us that the defense mechanism provides a positive improvement in the overall evacuation outcome.

We next look at the effect of different types of node misbehaviour on the dissemination of normal messages among non-malicious nodes. Figure 3a shows the number of created and received non-malicious EMs vs. number of malicious nodes. We see that drop-all behaviour does not affect the number of created normal messages (C), but that C increases under RF jamming and false info misbehaviours. This is because more CNs receive measurements from SNs in these cases due to misdirection (false info) and disrupted EM dissemination (RF jamming). We observe that the defense mechanism significantly increases the number of generated messages due to the use of blacklist messages (BMs), indicating a communication overhead. The number of received normal messages (R) is decreased with drop-all and RF jamming due to disruptions, but increased with false info without defense due to nodes staying longer in the building due to inefficient evacuation. The increase in R with the defense mechanism is due to a combination of nodes staying longer and to the increase in C due to BMs.

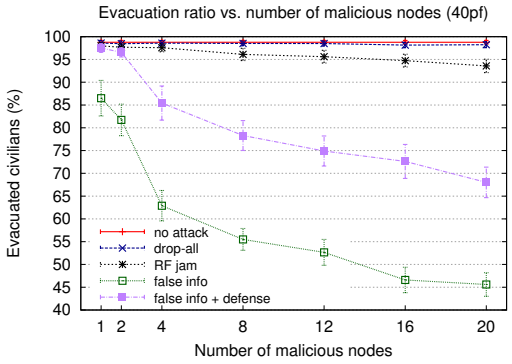
Figure 3b presents message delivery ratio for normal messages among non-malicious nodes, calculated considering the "one-to-all" dissemination of EMs and BMs. Drop-all misbehaviour does not affect delivery ratio much, indicating the resilience of oppcomms to such misbehaviour. Delivery ratio is significantly decreased by RF jamming and false info misbehaviours. As the number of malicious nodes increases, delivery ratio continues to decrease with RF jamming but it reaches a steady level with false info, with and without defense. We did not observe any significant effect of node misbehaviour on average message latency (not shown).

Average hop count of normal messages is given in Fig. 3c, which shows that hop count does not change much with drop-all and false info misbehaviours but decreases significantly as the number of malicious nodes increases with RF jamming. This indicates that RF jamming effectively partitions the oppnet into sub-networks which stay disconnected during evacuation, producing the resulting effect on hop count. This effect is especially apparent with higher number of misbehaving nodes, which increases partitioning of the oppnet.

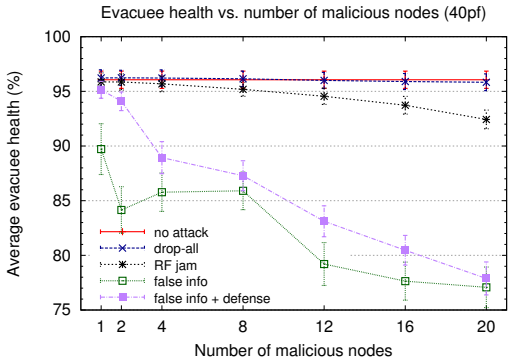
We finally look at the average of message queue usage in Fig. 3d, more specifically the average of the maximum storage (in number of packets) used by each CN for oppcomms. These results include malicious messages received by nodes for a more accurate representation of the effect of different misbehaviours on this metric. We observe that queue length is slightly lower than normal with drop-all behaviour, and RF jamming decreases queue length further by disrupting the dissemination of EMs by partitioning the oppnet. Queue length is significantly higher with false info behaviour due to the injection of malicious messages into the network. False info with defense has even higher queue lengths, which is mostly a result of overhead due to BMs.

Our results on evacuation outcome and communication performance show that although false info misbehaviour has the greatest impact on the evacuation, RF jamming has more impact on communications, but this effect translates weakly to degraded evacuation performance. These results also indicate that oppcomms is quite resilient to disruptions and especially to drop-all type of misbehaviour. Our proposed defense mechanism is able to improve evacuation performance considerably at the expense of some communication and storage overhead.

Figure 4 shows the performance of our detection mechanism in the identification of malicious nodes and packets with false info misbehaviour. As expected, the defense mechanism has no effect on the number of created malicious packets, but the ratio of created malicious packets to all created packets decreases with defense due to the creation of more normal messages, mostly BMs (see Fig. 4a). The number of malicious packets received by normal nodes is significantly reduced by the defense mechanism (see Fig. 4b), but as we discussed earlier, even a small number of received malicious packets has a great effect on evacuation. Figure 4c shows that around 65% to 70% of received malicious messages were correctly identified as such (labeled "detected pkts"), and a majority of the detected messages (between 80% and 90%) were identified before they were used to update the CNs and therefore had no direct effect on evacuation (labeled "dropped on receive"). The false positive ratio is generally

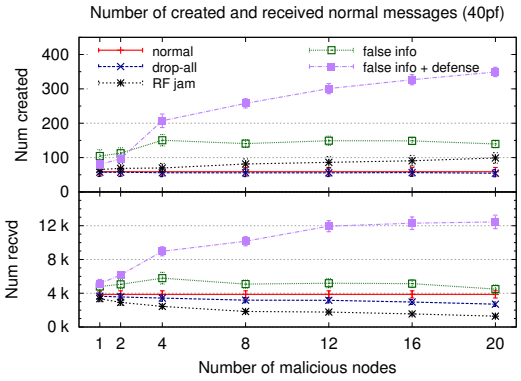


(a) Evacuation ratio

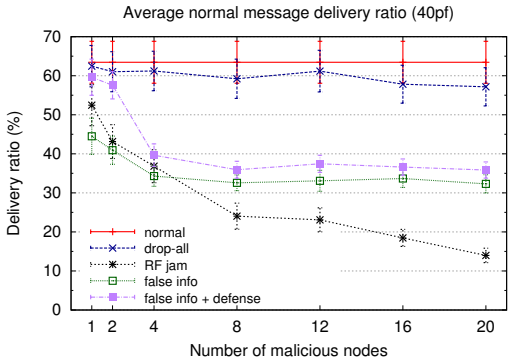


(b) Average evacuee health

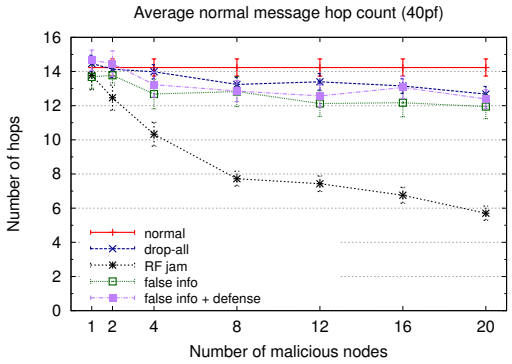
Figure 2: Evacuation performance under node misbehaviour



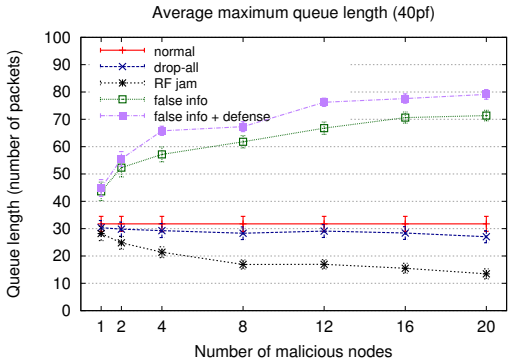
(a) Number of created and received normal messages



(b) Delivery ratio



(c) Hop count



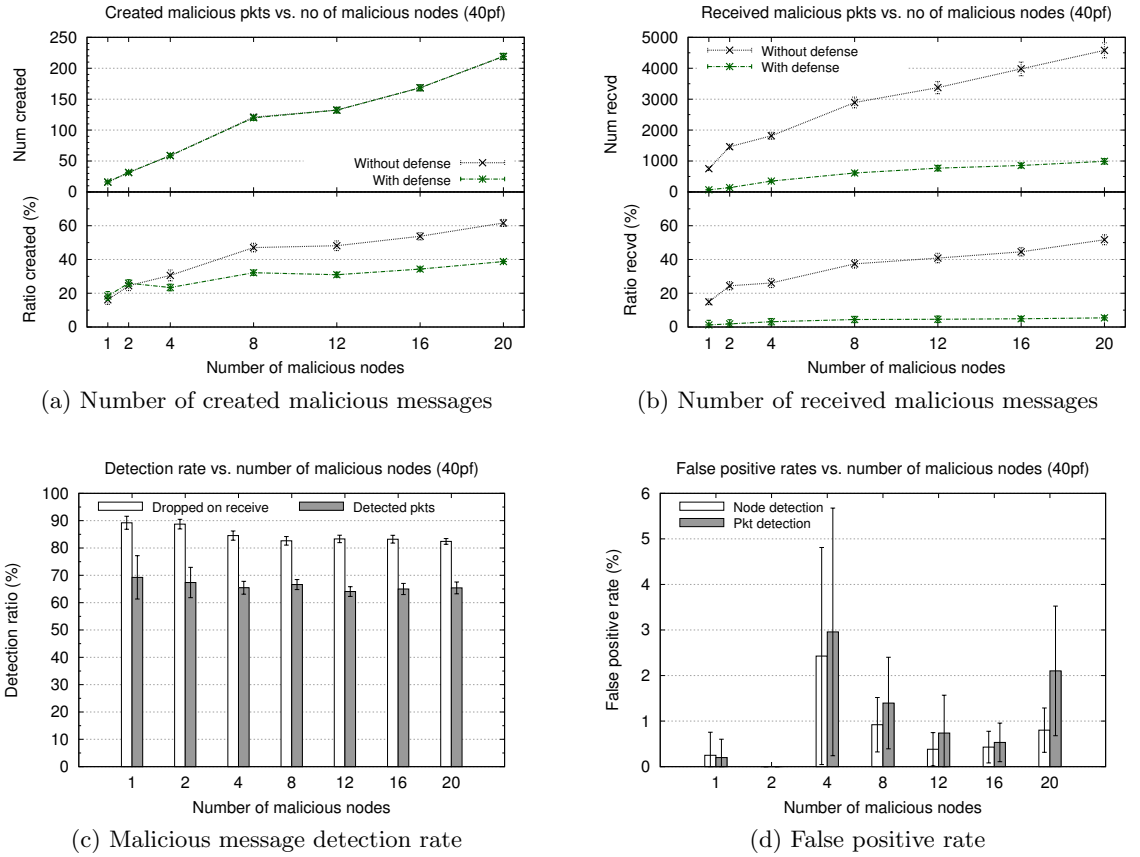
(d) Average maximum queue usage

Figure 3: Communication performance under node misbehaviour

quite low (between 0% and 3%) and the number of malicious nodes does not seem to have a consistent effect on this metric (see Fig. 4d). These results on detection performance indicate that although many of the malicious packets are correctly identified, the small number of remaining packets has a non-negligible effect on evacuation.

6. CONCLUSION

In this paper, we proposed the use of opportunistic communications to provide emergency evacuation support in built areas when other means of communication have broken down. We investigated the resilience and security of oppcomms as an enabler of emergency services considering the effect of different types of node misbehaviour. Our evaluation has shown that while oppcomms is quite resilient to disruptions, RF jamming and the generation of false messages to directly affect evacuation are two significant ways of attacking the network to affect communication and evacuation performance, respectively. We proposed a defense mechanism combining identity-based signatures and collective malicious packet detection based on content-based message verification. Our results show that the defense mech-



(a) Number of created malicious messages

(b) Number of received malicious messages

(c) Malicious message detection rate

(d) False positive rate

Figure 4: Performance of detection mechanism with false info misbehaviour

anism is able to detect a considerable amount of malicious packets with intermittent connectivity, and it improves evacuation outcome at the expense of some communication and storage overhead.

This paper has presented the role of number of misbehaving nodes in evacuation outcome and communication performance. We aim to investigate the effect of other parameters, such as population density and communication range, in future work where we would also consider issues of system oversight and data interpretation from incomplete information [18,19] as a way to evaluate the health of the system, as well as the use of classically used analytical techniques for performance evaluation [16,20], the challenges of managing old and new information that is gathered via oppcomms to evaluate the performance of the system as a whole, and the role of self-aware or autonomic means of managing the system as a whole and its network components [17]. The attack model we have considered only considers a small portion of all the possible attacks. Another relevant attack that we could consider would target the limited energy resources of network and sensor nodes.

Acknowledgements

The authors would like to acknowledge the support of the SATURN (Self-organizing Adaptive Technology underlying Resilient Networks) project which is sponsored by the UK Technology Strategy Board.

7. REFERENCES

[1] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo. Towards securing disruption-tolerant networking. Technical Report NRC-TR-2007-007, Nokia Research Center, Mar. 2007.

[2] E. Ayday, L. Hanseung, and F. Fekri. Trust management and adversary detection for delay tolerant networks. In *Proc. 2010 Military Comm. Conf.*, pages 1788–1793, 2010.

[3] M. Barnes, H. Leather, and D. K. Arvind. Emergency evacuation using wireless sensor networks. In *Proc. 32nd IEEE Conf. on Local Comp. Net.*, pages 851–857, Oct. 2007.

[4] R. Bruno, M. Conti, and A. Passarella. Opportunistic networking overlays for ICT services in crisis management. In *Proc. 5th Inter. ISCRAM Conf.*, pages 689–701, May 2008.

[5] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine. Surviving attacks on disruption-tolerant networks without authentication. In *Proc. 8th ACM Inter. Symp. on Mobile Ad Hoc Networking and Computing*, pages 61–70, 2007.

[6] D. Camara, C. Bonnet, and F. Filali. Propagation of public safety warning messages: A delay tolerant network approach. In *Proc. 2010 IEEE Wireless Communications and Networking Conf. (WCNC'10)*, pages 1–6, Apr. 2010.

[7] F. C. Choo, M. C. Chan, and E.-C. Chang. Robustness of DTN against routing attacks. In *Proc.*

2nd Inter. Conf. on Communication Systems and Networks, pages 1–10, 2010.

[8] N. Dimakis, A. Filippoupolitis, and E. Gelenbe. Distributed building evacuation simulator for smart emergency management. *The Computer Journal*, 53(9):1384–1400, 2010.

[9] J. Douceur. The Sybil attack. In *Peer-to-Peer Systems*, LNCS, pages 251–260. 2002.

[10] D. Elms, A. Buchanan, and J. Dusing. Modeling fire spread in buildings. *Fire Technology*, 20(1):11–19, 1984.

[11] K. Fall. A delay-tolerant network architecture for challenged internets. In *Proc. 2003 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03)*, pages 27–34. ACM, 2003.

[12] A. Filipoupolitis, G. Gorbil, and E. Gelenbe. Autonomous navigation systems for emergency management in buildings. In *Proc. 2011 IEEE GLOBECOM W'shops*, pages 1056–1061, Dec. 2011.

[13] A. Filippoupolitis. An adaptive system for movement decision support in building evacuation. In *Computer and Information Sciences*, volume 62 of *LNEE*, pages 389–392. 2010.

[14] A. Filippoupolitis and E. Gelenbe. A distributed decision support system for building evacuation. In *Proc. 2nd IEEE Inter. Conf. on Human System Interaction*, pages 323–330, May 2009.

[15] A. Filippoupolitis, G. Gorbil, and E. Gelenbe. Spatial computers for emergency support. *The Computer Journal*, 2012. doi: 10.1093/comjnl/bxs063.

[16] E. Gelenbe. A unified approach to the evaluation of a class of replacement algorithms. *IEEE Transactions on Computers*, 22(6):611–618, Jun. 1973.

[17] E. Gelenbe. Steps towards self-aware networks. *Communications of the ACM*, 52(7):66–75, Jul. 2009.

[18] E. Gelenbe and G. Hebrail. A probability model of uncertainty in data bases. In *Proc. 2nd Inter. Conf. on Data Engineering (ICDE'86)*, pages 328–333, Feb. 1986.

[19] E. Gelenbe and L. Hey. Quality of information: An emprical approach. In *Proc. 5th IEEE Inter. Conf. on Mobile Ad-Hoc and Sensor Systems*, pages 730–735, Oct. 2008.

[20] E. Gelenbe and A. Stafylopatis. Global behaviour of homogeneous random neural systems. *Applied Mathematical Computing*, 15(10):534–541, 1991.

[21] G. Gorbil, A. Filippoupolitis, and E. Gelenbe. Intelligent navigation systems for building evacuation. In *Computer and Information Sciences II*, LNEE, pages 339–345. Springer London, 2012.

[22] G. Gorbil and E. Gelenbe. Opportunistic communications for emergency support systems. *Procedia Computer Science*, 5:39–47, 2011.

[23] Y. Inoue, A. Sashima, T. Ikeda, and K. Kurumatani. Indoor emergency evacuation service on autonomous navigation system using mobile phone. In *Proc. 2nd Inter. Symp. on Universal Communication*, pages 79–85, Dec. 2008.

[24] P. Jiang, J. Bigham, and E. Bodanese. Adaptive service provisioning for emergency communications with DTN. In *Proc. 2011 IEEE Wireless Communications and Networking Conf. (WCNC'11)*, pages 2125–2130, Mar. 2011.

[25] S. Li, A. Zhan, X. Wu, and G. Chen. ERN: Emergency rescue navigation with wireless sensor networks. In *Proc. 15th Inter. Conf. on Parallel and Distributed Systems (ICPADS'09)*, pages 361–368, Dec. 2009.

[26] D. Ma and G. Tsudik. Security and privacy in emerging networks. *IEEE Wireless Communications*, 17(5):12–21, Oct. 2010.

[27] M.-S. Pan, C.-H. Tsai, and Y.-C. Tseng. Emergency guiding and monitoring applications in indoor 3D environments by wireless sensor networks. *International Journal of Sensor Networks*, 1(1/2):2–10, Jan. 2006.

[28] L. Pelusi, A. Passarella, and M. Conti. Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks. *IEEE Communications Magazine*, 44(11):134–141, Nov. 2006.

[29] A. Seth and S. Keshav. Practical security for disconnected nodes. In *Proc. 1st IEEE ICNP W'shop on Secure Network Protocols (NPSec'05)*, pages 31–36, Nov. 2005.

[30] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology (CRYPTO'84)*, LNCS, pages 47–53. 1984.

[31] L. Song and D. F. Kotz. Evaluating opportunistic routing protocols with large realistic contact traces. In *Proc. 2nd ACM W'shop on Challenged Networks (CHANTS'07)*, pages 35–42. ACM, 2007.

[32] Y.-C. Tseng, M.-S. Pan, and Y.-Y. Tsai. Wireless sensor networks for emergency navigation. *IEEE Computer*, 39(7):55–62, Jul. 2006.

[33] Y. S. Uddin, A. Khurshid, H. D. Jung, C. Gunter, M. Caesar, and T. Abdelzaher. Making DTNs robust against spoofing attacks with localized countermeasures. In *Proc. 8th Ann. IEEE Comm. Soc. Conf. on Sensor, Mesh and Ad Hoc Comm. and Net.*, pages 1–9, Jun. 2011.

[34] A. Vahdat and D. Becker. Epidemic routing for partially-connected ad hoc networks. Tech. Report CS-2000-06, Duke Univ. CS Dept., Apr. 2000.

[35] W. van Willigen, R. Neef, A. van Lieburg, and M. C. Schut. WILLEM: A wireless intelligent evacuation method. In *Proc. 3rd Inter. Conf. on Sensor Technologies and Applications (SENSORCOMM'09)*, pages 382–387, Jun. 2009.

[36] S. Winter, K.-F. Richter, M. Shi, and H.-S. Gan. Get me out of here: Collaborative evacuation based on local knowledge. In *Proc. 3rd ACM SIGSPATIAL Inter. W'shop on Indoor Spatial Awareness*, pages 35–42, Nov. 2011.

[37] X. Wu, M. Mazurowski, Z. Chen, and N. Meratnia. Emergency message dissemination system for smartphones during natural disasters. In *Proc. 11th Inter. Conf. on ITS Telecommunications (ITST'11)*, pages 258–263, Aug. 2011.