SURVEY PAPER

A SURVEY OF THE ULTIMATE SECURITY SOLUTION IN OPPORTUNISTIC NETWORK: TRUST MANAGEMENT

By

BASIRA YAHAYA *

MOHAMMED BASHIR MUAZU **

EMMANUEL ADEWALE ADEDOKUN ***

IME J. UMOH ****

*-**** Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

Date Received: 11/01/2019 Date Revised: 06/02/2019 Date Accepted: 25/03/2019

ABSTRACT

Opportunistic network (oppnets) is a promising paradigm, which allows communication to be set up between nodes even without infrastructure in a delay tolerant fashion. It has even become more pertinent with the proliferation of varieties of autonomous mobile devices. However, malicious devices pose potential security threats (packet dropping, eavesdropping, Denial of Service (DoS) attack, black hole attack, Identification (ID) spoofing, etc.) to the performance of oppnets, due to the inherent characteristics of such networks like ever changing network topology and lack of a definite communication path between nodes amongst others. Recent focus on mitigation mechanisms for security threats in oppnets is on trust management since various mechanisms have been used, but the trust-based methods appeared to meet up with the security requirement of the opportunistic network better. However, no work strictly present trust management extensively. This paper presents trust management together with trust related issues in oppnet (trust-based security threats, trust mechanism, and the trust management scheme as oppnet security solution). It is aimed at providing the reader a clear understanding of trust management (preferred solution) within a single literature.

Keywords: Opportunistic Networks, Security, Trust Management, Privacy, Security Threats.

INTRODUCTION

The opportunistic network is a connection of nodes that communicate over an almost bandwidth-constrained wireless networks. Opportunistic network is a type of self-organizing delay tolerant networks with several wireless nodes opportunistically communicating with one another in a "Store–Carry–Forward" manner. According to Kaur and Kaur (2009); Verma and Srivastava (2012), it has the following basic features:

- It consists of wirelessly connected nodes that are mobile or steady (a node is any device that is joined to a network and has the ability of receiving, sending, or forwarding information over communication medium).
- A complete end-to-end path between two nodes intending to communicate is not available.
- Its communication range is not fixed, as it consists of different types of heterogeneous nodes.
- Its communication paths are dynamically built; any node can be used as the next hop as long as it is likely to bring the message closer to its ultimate destination.
- Network topology is unstable as it can change at any given point of time.

Oppnets, due to their flexibility and ease of deployment, are fast gaining grounds as networks of choice in emergency services, military operations, network expansion, etc., especially in difficult environments where infrastructure do not exist. However, because there is no guaranteed end-to-end connectivity, the possibility of oppnets being joined by malicious nodes thereby threatening the confidentiality and integrity of data is a critical one and a limiting factor to their widespread use.

Since a complete path between two nodes intending to communicate is not available, there is the problem of lack of complete connectivity in an oppnet, which makes it impossible to make direct initial authentication from a sending node to a destination node. Without initial authentication, malicious devices join the oppnet causing different forms of security threats. These malicious devices receive and drop packets at will, masquerade themselves and steal or temper with messages meant for other nodes, exaggerate the trust value of other malicious devices or lower the trust value of a trusted node amongst others. These behaviors could lead to loss of packets, increase in delay of message transmission, breach of privacy, compromising data confidentiality and integrity, and eventually, decrease in performance of the network evident from a decrease in delivery probability (Barai & Bhaumik, 2016). As such, security consideration is a critical issue in oppnet routing protocol.

Various mechanisms have been used to address security issues in the oppnet. Due to the aforementioned oppnet characteristics/features, most mechanisms (cryptography, intrusion detector, etc.) are found wanting in one way or the other. The trust-based schemes appeared to be the preferred security mechanisms for oppnet because it suits the characteristics of oppnet better (Barai & Bhaumik, 2016). However, no literature extensively concentrates on trust management and related trust issue for oppnet. This survey presents the trust management scheme as the ultimate security solution for oppnet.

1. Related Works on Security Solution in Opportunistic Networks

Some works carried out in order to address security issues in oppnet are shown in Table 1.

Trust management is able to meet the security requirements in the opportunistic networks, which include; authentication, authorization, access control, data confidentiality, data integrity, privacy protection, and node cooperation (Wu, Zhao, Riguidel, Wang, & Yi, 2015).

2. Security Mechanisms in the Opportunistic Networks

Various mechanisms have been used to address security issues in oppnets, classified as trust-based and privacy-based protocols. The trust-based protocols are further divided into friend-vector based, familiarity-based, reputation based, and hybrid-trust based. On the other hand, the privacy-based protocols are divided into cryptography-based and cryptography-free as depicted in Figure 1 (Barai & Bhaumik, 2016).

Another classification for the trust-based protocol has three types: social trust, environmental trust, and similarity trust as depicted in Figure 2 (Trifunovic & Legendre, 2009). This classification presented the security mechanism as trust-based and cryptography-based.

Proposed Model	Limitations
Intrusion Detector (Kaur & Kaur, 2009)	The intrusion detector is not a good security check in the oppnet due to the heterogeneous nature oppnet
Cryptographical means (Shikfa, 2010)	Cryptography-based algorithms are not suitable in oppnets because they require very complex and computationally intensive operations in order to obtain the required level of protection
Trust metric (Poonguzharselvi & Vetriselvi, 2012)	Assumed Trust threshold value
Cluster estimation based on cryptography (Goyal & Chaudhary, 2013)	Cryptography-based algorithms are not suitable in oppnets because they require very complex and computationally intensive operations in order to obtain the required level of protection
Trust-based security protocol (Gupta, Dhurandher, Woungang, Kumar, & Obaidat, 2013)	Failure to consider a dynamic function in calculating the social group value (SGV) of randomized malicious behavior of nodes. Also, they did not optimally select a trust threshold value for their protocol
Intrusion Detector (Alajeely, Doss, & Ahmad, 2016)	The intrusion detector do not perform well in oppnet due to its nature of attacks and the heterogeneous nature of oppnet
Trust metric (Xi, Liang, Feng, & Zhuo, 2015).	Assumed Trust threshold value
Cyber foraging based on cryptography (Padhi, Tiwary, Priyadarshini, Panigrahi, & Misra, 2016)	Cryptography-based algorithms are not suitable in oppnets because they require computationally intensive operations that most oppnet node cannot handle
Trust metric (Yao, Man, Huang, Deng, & Wang, 2016)	The strong assumption that users are willing to share their social features, which is not always the case in real life due to privacy related issues
Trust-based (Kungwani & Dudhe, 2016)	The K Nearest Neighbor (KNN) algorithm used in trust scheme made it application difficult in oppnet

Table 1. Reviews of Security Solution in Opportunistic Networks

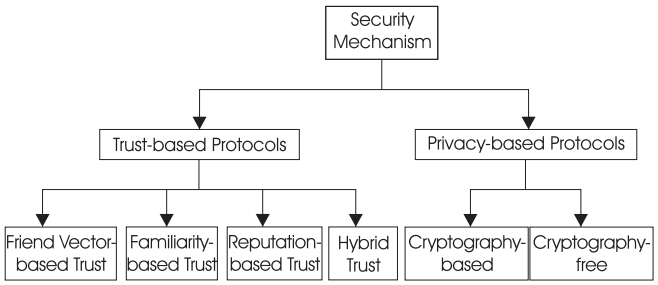

Figure 1. Taxonomy of Security Mechanisms in Oppnets (Barai & Bhaumik, 2016)

Due to the characteristics of oppnets (lack of end-to-end connectivity, unstable structure, etc.), cryptography-based schemes (Shikfa, 2010; Padhi et al., 2016) are unsuitable because nodes depend mainly on the next hop in order to forward data. This informed the need for a security mechanism which would ensure that the intermediate nodes do not behave maliciously. Cryptography-based algorithms are also not well realizable in oppnets because they require very complex and computationally intensive operations in order to obtain the required level of protection. Most devices in oppnets are made to be portable and energy efficient and as such even have less powerful hardware than those contained in conventional Personal Computers (PCs) (Xi et al., 2015; Trifunovic & Legendre, 2009; Barai & Bhaumik, 2016). In view of these, the trust-based schemes are the preferred security mechanisms for oppnets.

The trust management schemes (Trifunovic & Legendre, 2009; Xi et al., 2015; Chang, Chen, Bao, & Cho, 2011; Poonguzharselvi & Vetriselvi, 2012; Chen, Bao, Chang, & Cho, 2014; Gupta et al., 2013; Indikar, & Kattimani, 2015; Khot & Mogal, 2017; Singh & Chawla, 2014) are dependent of the computation of trust values (which represent the trustworthiness of a node in the network). The establishment of trust will validate a nodes' legitimacy and refuse malicious nodes better in oppnets. However, the efficiency of the trust algorithms depends on what basic framework is followed in calculating the trust oppnets (Xi et al., 2015; Trifunovic & Legendre, 2009; Barai & Bhaumik, 2016). In order to use trust mechanism, attempt should be made for choosing the best trust threshold value.

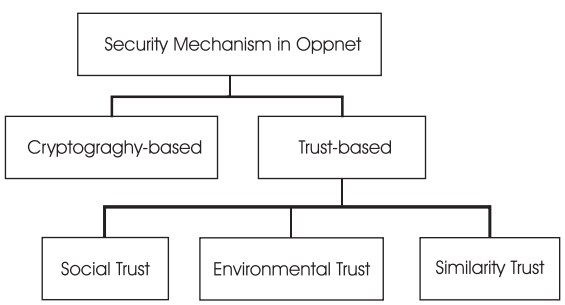

Figure 2. Security Mechanisms in Oppnets (Trifunovic & Legendre, 2009)

3. Trust-Related Attacks in the Opportunistic Networks

A malicious (compromised) node aims to distort the performance of the opportunistic routing process. It drops packet at will and performs these trust-related attacks (Balaganesh & Nalini, 2014; Indikar & Kattimani, 2015):

3.1 Self-Promoting Attack

In order to attract packets to itself, the malicious node boosts its importance in the network by giving good recommendations for itself. It portrays itself as having the highest probability or shortest path to the required destination. Afterwards, it performs malicious act by dropping or consuming the packet without forwarding it.

3.2 Bad-Mouthing Attack

Malicious nodes provide false negative recommendation of well-behaved nodes so as to spoil the reputation of the well-behaved node. By so doing, messages are not forwarded to the trusted nodes as they have been blackmailed. This greatly affects the routing performance since the actual candidates are not used.

3.3 Ballot Stuffing

Malicious nodes give good recommendation of other malicious node thereby, boosting their reputation. This is done in order to encourage the use of these malicious node forwarding process. Once these malicious nodes are employed, they perform their notorious act.

A malicious node also has the ability to perform random attacks to prevent detection. A malicious node has the ability to also perform all the three trust related attacks. Ballot stuffing and bad-mouthing attacks are called collaborative/joint attack, i.e malicious nodes increase the reputation of their allies and decrease the reputation of good nodes.

4. Trust Management

Trust is an indication of a device's faithfulness and a measure of the quality of service that the device can render, which is sometimes interchanged with reputation. However, reputation has to do with the perception regarding a nodes' behavior, which must be held by other nodes, based on experience and observation of its past actions. i.e., reputation is evaluated based a second agent's perception. Trust management is a process of evaluating, collecting, and propagating trust in a network. Trust management are built using trust algorithms. It evaluates the level of trust between nodes in order to obtain the required availability of oppnet and to resist malicious packet dropping. A good trust management scheme should ensure that the security requirements (access control, data confidentiality, data integrity, privacy protection, cooperation as well as proper authorization) of the oppnet are met. Different forms of trust exist in order to fit different scenarios (Wu et al., 2015; Trifunovic & Legendre, 2009). These include (Trifunovic & Legendre, 2009) the following.

4.1 Social Trust

A secured and reliable friend ties (common friends, common interest) can be achieved from a proper understanding of the mobility pattern of devices. Friends list are exchanged and saved whenever a node is encountered. This is used in creating a friendship graph (friendship graph is designed in levels constituted by a set of nodes with the same distance from a local node, where edges exist between nodes in sequenced levels only). Trust is evaluated as function of hop distance (they share an inverse relationship) and positive recommendations from other nodes (they share a direct relationship). A transitivity of trust is assumed over a reasonable distance (up to six hops). A peer initially has to asks its friends for opinion before working with an unknown peer. Friends inform each other whenever a malicious peer is detected in the network in order to eliminate the malicious peer. Trust and recommendation values are defined by probability. There are advantages and disadvantages of taking friends connections as a basis of establishing trust. Sybil attacks is prevented by secured pairing process, where the node entity behind the identity is justified. On the other hand, the transitivity of trust allows a Sybil attacker to only need to create one trusted relation in order to acquire the required trust of other nodes. Also, the friendship graph is loosely connected and does not guarantee a regular interaction. As such, trust assessment of nodes that are met regularly is not guaranteed.

4.2 Environmental Trust

This is called familiarity based models in some literatures (Barai & Bhaumik, 2016). There are certain people we regularly share the same activity or the same space in our everyday life (for example, the same coworker sharing the same office every day, people living in the same building apartment or estate, people who regularly go to the same mosque, attend the same church or regularly visit a particular location (say gymnasium) at a particular time). These communities can be identified using a community detection algorithm that carefully observe the interested environment and analyze the categories of peers in the area over time. Social notion is not guaranteed here since member of the community may not know each other, or be friends with each other, but share the same space for a significant length of time. This method has an advantage of not relying on users' interaction over the friends-based social trust. Also, a given level of trust in a well-known or familiar stranger can be justified, which is useful for preventing Sybil attack. However, this method is not as secured as the social trust since community detection cannot guarantee a certain entity as the proclaimed identity. Also, more care is needed in making the current community detection mechanisms resilient to attacks since they are easily tempered with.

4.3 Similarity Trust

The comparison of the recommendation of other users with direct experience is used to assess trust on similarity interest. It is seen as part of a reputation system and it is called the reputation based trust in some literatures (Alajeely, Doss & Ahmad, 2016; Barai & Bhaumik, 2016). This trust might identify an unwanted entity or select peers, which due to their similar taste are more relevant in a given scenario. Making similarity trust a secured way of

assessing trust is difficult in oppnet because:

- It requires a reputation system and users need to have experience.
- In a decentralized environment, recommendations can be forged easily and changed to be similar with targeted peer.
- Data-centric Trust: the aforementioned trust notions are entity-centric (trust taken as a relation between entities) are slow to change. Oppnet systems are data-dependent in their functionality and usually operate in an unstable manner. As such, it is worthy to create trust in data rather than the nodes reporting them. Also, nodes can be faulty, unreliable, and insufficiently equipped for data in the network (Wu et al., 2015).
- Hybrid Trust: this model is a combination of two or more of the aforementioned trusts. For example, social studies have shown that people in close proximity tend to have some similarities with one another. People tend to socialize, communicate, cooperate, and potentially trust each other if they belong to the same community of interest or activity.

5. Trust Management Scheme for Security in the Opportunistic Network

Xi et al. (2015) presented a trust management scheme that used feedback information propagated by other nodes, which uses a social context-based key management algorithm. By using the social context information, mobile nodes can issue and exchange certificate with each other. This gives the mobile node the opportunity to query the validity of a certificate path for the nodes they encounter in less time. Certificate is issued only between nodes with reasonably high similar social attributes. This is so in order to reduce the storage needed by each nodes certificate sub graph. The trust model considered four basic components (Oppnet trust model, social context-based key management, secured forwarding, and feedback system) as depicted in Figure 3.

Each node generates its Public Key (PK) and private key (SK) pairs. Mobile nodes can share their public keys with others efficiently based on the social-based key management. This guarantees nodes' mutual authentication and message privacy and confidentiality. In order to check packet dropping by malicious node, secured forwarding based on Verifiable Feedback Packets (VFP) was introduced. These VPF are used to deal with the trust related security attacks in the oppnet because a VPF is generated after a node performs a positive behavior. The trust management scheme defined two types of trust; namely identity trust and behavioral trust. Identity trust between two nodes (say a and b) implies that they can authenticate each other by their public and private key pairs. That is, the existence of identity trust between two nodes ensures security of transmitting and forwarding message. Behavior trust is based on VFP propagation. If b has enough valid and verifiable VFP's of a, then b's behavior trust a. Large VFP is an indication that a node helps in forwarding a lot of messages, implying that it is not a malicious node that drops packets. The key management system issues, exchange, update, and revoke certificates are presented as follows (Xi et al., 2015):

5.1 Certificate Issue

When a node comes in communication range with another node, they issue certificate to each other if their identities are trusted. The certificate is given to a new node

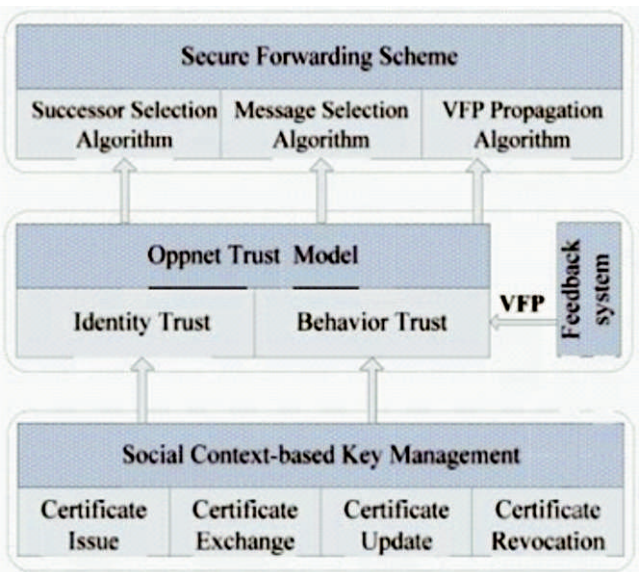

Figure 3. Model of the Trust Management Scheme (Alajeely et al., 2016)

if the match in attribute (between the two meeting nodes) is greater than a fixed threshold value. The certificate is an indication that the nodes trust the authenticity of one another. The certificate is given a period of validity and a reliability value, then signed by the giver of the certificate.

5.2 Certificate Exchange

During the period of warm up, nodes exchange their certificate database with each qualified encountered node in order to gather as many certificates as possible. At on-stream period, nodes only exchange certificate information with other encountered nodes whose match of social attribute is greater than a given threshold value.

5.3 Certificate Revocation

Certificates are revoked whenever the private key of a mobile node leaks, or the binding ability of a nodes' private key and public key has changed. A certificate can be revoked by both the giver of the certificate and the owner of the certificate. The certificate revocation information has the highest preference in the network traffic in order to notify other node who may also possess the certificate.

The feedback system is used to screen nodes based on the reputation. Whenever a node behaves positively, it is issued a VFP. When a node has certain number of VFP, it is an indication that the node is not a malicious node. Successor selection algorithm is used to ensure that a message is not forwarded to a malicious node while message selection algorithm is used to ensure that a malicious message (which is capable of overworking a node or causing denial of service attack) is not accepted by any node. This trust management scheme ensures that malicious nodes are kept out of the network as such, message confidentiality, integrity, and privacy are achieved.

5.4 Certificate Update

When the validity period of a certificate expires, the giver of the certificate will have to wait for another encounter to repeat the process of certificate issue.

Conclusion

Opportunistic networks have the potential of complementing (or even replacing) the traditional wired and wireless networks due to their ease of deployment, non-reliance on any central administration nor dependence on any pre-existing infrastructure. However, security and privacy issues pose serious challenges to this promising technology thereby, limiting their performance and widespread use. Various mechanisms have been used to address security issues in the opportunistic network. The trust-based schemes appeared to be the preferred security mechanisms for opportunistic network. This is because trust mechanisms are able to deal with the security requirements for the opportunistic network effectively. Trust management and trust related issues (threats based on trust) are presented in this survey, intended to provide a clear understanding of trust management as the preferred method of solving security issue in oppnet. As future work, emphasis should be laid on how trust algorithm should select trust threshold value because of its importance to the performance of the opportunistic networks.

References

[1]. Alajeely, M., Doss, R., & Ahmad, A. A. (2016). Security and trust in opportunistic networks–a survey. *IETE Technical Review*, 33(3), 256-268.

[2]. Balaganesh, M., & Nalini, N. (2014). A survey of trust based automatic routing in delay tolerant networks. *International Journal of Advanced Information Science and Technology*. 3, 51-54.

[3]. Barai, S., & Bhaumik, P. (2016). A taxonomy of recent security concerns in opportunistic networks. *International Journal for Scientific Research & Development*, 1, 34-46.

[4]. Chang, M., Chen, R., Bao, F., & Cho, J. H. (2011). Trust-threshold based routing in delay tolerant networks. In *IFIP International Conference on Trust Management* (pp. 265-276). Springer, Berlin, Heidelberg.

[5]. 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.

[6]. Goyal, M., & Chaudhary, M. (2013). Ensuring privacy in opportunistic network. *IOSR Journal Computer Engineering*, 13(2), 74-82.

[7]. Gupta, S., Dhurandher, S. K., Woungang, I., Kumar, A., & Obaidat, M. S. (2013). Trust-based security protocol against blackhole attacks in opportunistic networks. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on* (pp. 724-729). IEEE.

[8]. Indikar, N. J & Kattimani L. S. (2015). Dynamic trust and security management protocol for delay tolerant networks using information centric-Networks Architecture. *International Journal of Engineering And Computer Science*, 4(6), 12698-12704.

[9]. Kaur, E. U., & Kaur, E. H. (2009). Routing techniques for opportunistic networks and security issues. In *National Conference on Computing, Communication and Control (CCC)* (Vol. 9, No. 2009, pp. 155-161).

[10]. Khot, A., & Mogal, V. (2017). Trust preservation in opportunistic networks. *International Journal of Innovative Research in Computer and Communication Engineering*, 5, 2489-2494.

[11]. Kungwani, B., & Dudhe, P. (2016). Trust based privacy preserving Friend recommendation in social network web. *International Journal of Research in Science & Engineering*, 2(5), 38-43.

[12]. Padhi, S., Tiwary, M., Priyadarshini, R., Panigrahi, C. R., & Misra, R. (2016). SecOMN: Improved security approach for Opportunistic Mobile Networks using cyber foraging. In *Recent Advances in Information Technology (RAIT), 2016 3rd International Conference on* (pp. 415-421).

[13]. Poonguzharselvi, B., & Vetriselvi, V. (2012). Trust framework for data forwarding in opportunistic networks using mobile traces. *International Journal of Wireless & Mobile Networks*, 4(6), 115.

[14]. Shikfa, A. (2010). Security issues in opportunistic networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking* (pp. 215-216). ACM.

[15]. Singh, R., & Chawla, M. (2014). An efficient trust management technique for delay tolerant network. *International Journal of Computer Applications*, 98(21) 8-12.

[16]. Trifunovic, S., & Legendre, F. (2009). Trust in opportunistic networks. *Computer Engineering and Network Laboratory, ETH Zurich,* Switzerland.

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

[18]. 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.

[19]. Xi, C., Liang, S., Feng, M. A. J., & Zhuo, M. A. (2015). A trust management scheme based on behavior feedback for opportunistic networks. *China Communications*, 12(4), 117-129.

[20]. Yao, L., Man, Y., Huang, Z., Deng, J., & Wang, X. (2016). Secure routing based on social similarity in opportunistic networks. *IEEE Transactions on Wireless Communications*, 15(1), 594-605.

ABOUT THE AUTHORS

Dr. Basira Yahaya is currently a Lecturer in Ahmadu Bello University, Zaria, Nigeria. She received her B.Eng Degree in Electrical Engineering from Ahmadu Bello University (ABU), Nigeria in 2011, and an MSc., and PhD. in Computer Engineering from same University (ABU) in 2015 and 2018, respectively. Her research interests are in the areas of Networking, IoTs, and Cloud Computing.

Mohammed Bashir Muazu is working in the Department of Computer Engineering at Ahmadu Bello University, Zaria, Nigeria.

Emmanuel Adewale Adedokun is working in the Department of Computer Engineering at Ahmadu Bello University, Zaria, Nigeria.

Dr. Ime J. Umoh is a Faculty member at Ahmadu Bello University. He obtained his Ph.D at University of Southampton in Graphene Device Modelling, and M.Sc in Microelectronics Systems Design at University of Southampton. His current research is focused on implementation of Opportunistic Networks.