DRAFT: Trust Framework Operation in Autonomous Marine Communications Environments

In Preparation for Submission Ad-Hoc Now 2015, Athens, June 29 - July 02 2015. Deadline 07 Feb 2015

Andrew Bolster[*] , Alan Marshall, Ji Guo

Advanced Networks Research Group,
Department of Electrical Engineering & Electronics,
University of Liverpool, UK
{andrew.bolster,alan.marshall}@liv.ac.uk
http://www.anrg.liv.ac.uk/

[*] Please note that the LNCS Editorial assumes that all authors have used the western naming convention, with given names preceding surnames. This determines the structure of the names in the running heads and the author index.

Table of Contents

Abstract. This paper presents a Trust Management Framework (TMF) for Marine Autonomous Networks, including a critique of previous group work in this area utilising Fuzzy Sets and Gray Theory. We present a comparative study on the operation and performance of such trust frameworks between the terrestrial and the harsh underwater communications environments. We demonstrate the need for a different approach towards metric selection and trust-timing in such constrained networks.

Keywords: ad-hoc, MANET, trust, marine, underwater, acoustic

1 Introduction

As mobile ad-hoc networks (MANETs) grow beyond the terrestrial arena, their operation and the protocols designed around them must be reviewed to assess their suitability and optimality in different communications environments to ensure their continued security, reliability, and performance.

Trust Management Frameworks (TMFs) provide information to assist the estimation of future states and operations of nodes within networks. This information is used to optimize the performance of a system of systems in the face of malicious, selfish, or defective behavior by one or more nodes within such a system. Previous research has established the advantages of implementing distributed TMFs in terrestrial, 802.11 based mobile ad-hoc networks (MANETs), particularly in terms of preventing selfish operation in constrained collaborative systems [Li and Singhal, 2007], and maintaining throughput in the presence of malicious actors [Buchegger and Le Boudec, 2002]

Current TMFs generally use a single type of observed action to derive trust metrics, i.e. successfully forwarded packets. These historical observations then inform future decisions of individual nodes, for example, the selection of a forward router with the lowest previous Packet Loss Rate (PLR) [Li et al., 2007].

Recent work has demonstrated the use of a number of metrics together, forming a vector of trust. In the case of [Guo, 2012], these metrics related to inter-node communications. This vectorized trust allows a system to detect anomalous behavior and identify the tactics being used to undermine or subvert trust.

However, this work has been limited to terrestrial, RF based, communications networks. As Autonomous underwater vehicles (AUVs) become more capable, and economical, they are being used in a many defence, commercial and environmental applications. These applications are tending towards utilising independent collective behaviour of teams or fleets of these platforms [Caiti, 2011] With this use being increasingly independent of classical command and control structures, the accurate and timely establishment of mutual and distributed communications trust between nodes within such fleets is essential for the reliability and stability of such systems, and to the secure integration of such systems into larger management systems-of-systems.

As such, the application of Trust methods developed in the Terrestrial MANET space must be re-appraised for application within the challenging underwater communications channel.

1.1 Paper Structure

In section 2 we discuss Trust and Trust Management Frameworks, defining our terminology and reviewing the justifications for the use and development of Trust Management Frameworks. We then review the results presented in [Guo et al., 2011] and discuss the differences in experimental setup when transitioning to the marine space. In section 3, we review selected features of the underwater communications channel, highlighting particular challenges and differentials against terrestrial equivalents. In section 4 we establish the initial parameters for simulation and set out a series of experiments to establish commonality between trust establishment in Terrestrial and Marine networks, characterising the communications and physical configuration with respect to the application and channel characteristics. In section **??**, we present our findings in trust establishment in this optimal network, pointing out the differences in metric selection and their impact on trust assessment stability.

1.2 Contributions

- A Trust Management Framework applicable to Underwater MANETs.
- A study on the comparitive operation and performance between Terrestrial and Underwater MANETs.

- A review of metric suitability for Trust Management Frameworks in Marine Environments, informing future metric selection for experimenters and theorists.

2 Trust and Trust Management Frameworks

2.1 Trust in MANETs

In human trust relationships it can be seen that there can be several perspectives of Trust for example organizational, sociological, interpersonal, psychological and neurological [Lee and See, 2004].

For the purposes of this work we define two perspectives on trust for autonomous systems: Design and Operational. These are summarised as follows:

- *Design Trust*; When an autonomous system is under development a level of Trust is established in it through the manner in which it has been designed and tested. This is the same as conventional systems. The difference with systems that have high-levels of autonomy is that they are designed to behave adaptively to dynamic environments that are difficult to fully predict prior to operational deployment. For example, in a navigation system it is difficult to predict the dynamic environment it will need to adapt to. So Trust needs to be developed that the design and test of such systems are sufficient to predict that operation will be, if not optimal, at least satisfactory.
- *Operational Trust*; Trust at runtime or in-situ that both the individual nodes within a system are operating as expected[1]; and that the interfaces between the operator and the system are as expected. This latter aspect covers issues such as physical/wireless links and interpretation of data at each end of such a communication link.

In addition to the two perspectives of trust identified, it is necessary to define and classify Operational Trust into two distinct but related sections, which we define as being:

- *Hard Trust* or technical trust, being the quantitative measurement and communication of the expectation of an actor performing a certain task, based on historic performance and through consensus building within a networked system. Can be thought of as a de-risking strategy to measure and monitor the ability of a system, or another actor within a system, to perform a task unsupervised.
- *Soft Trust* or common trust, being the qualitative assessment of the ability of an actor to perform a task or operation consistently and reliably based on social or experiential factors. This is the natural form of trust and is the main motivational driver for the human-factors trust discussion. Can be rephrased as the level of confidence an operator has in an actor to perform a task unsupervised.

[1] Operational Trust is functionally derived from, but distinct from Design Trust

For the purposes of this work, we are concerned with the analytical establishment of hard trust within a topologically dynamic network of autonomous actors.

2.2 Current Trust Management Frameworks

Various models and algorithms for describing trust and developing trust management in distributed systems, P2P communities or wireless networks have been considered. Taking two examples;

- *The Objective Trust Management Framework* takes a Bayesian network approach and introduces the idea of applying a Beta function to changes in the per-link Packet Loss Rate (PLR) over time as an encapsulation method, combining "Trust" and "Confidence of Assessment" into a single value [Li et al., 2007]. OTMF however does not appropriately combat multi-node-collusion in the network [Cho et al., 2011].
- *Trust-based Secure Routing [Moe et al., 2008]* demonstrated an extension to Dynamic Source Routing (DSR), incorporating a Hidden Markov Model of the wider ad-hoc network, reducing the efficacy of Byzantine attacks, particularly black-hole attacks but, along with many more TMFs surveyed in [Cho et al., 2011], falls under the same limitation of focusing on single metric observation (PLR).
- *CONFIDANCE*; **DRAFT: Add [Buchegger and Le Boudec, 2002] in here if there's space, or find something more recent built on it**

These single metric TMFs provide malicious actors with a significant advantage if their activity is undetectable by that one assessed metric, especially if the attacker knows the metric in advance.

The objective of operating a TMF is to increase the confidence in, and efficiency of, a system by reducing the amount of undetectable negative operations an attacker can perform. This space of potential attacks can be described as the Threat Surface. In the case where the attacker can subvert the TMF, the metric under assessment by that TMF does not cover the threat mounted by the attacker. In turn, this causes a super-linearly negative effect in the efficiency of the network as the TMF is assumed to have reduced the threat surface when in fact it has only made it more advantageous to attack a facet of the networks operation. [Huang et al., 2010] also raised the need for a more expanded view of trust but did so with a domain-partitioning approach rather than combining trust assessments from multiple domains within networks.

2.3 Grey Relational Trust for Terrestrial MANETs

[Guo, 2012] demonstrated the ability of Grey Relational Analysis (GRA)[Zuo, 1995] to normalize and operationally combine disparate traits of a communications link such as instantaneous throughput, received signal strength, etc. into a single comparable value, a Grey Relational Coefficient, or a "trust vector". This vector is given

$$\theta^t_{k,j} = \frac{\min_k |a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|}{|a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|} \tag{1}$$

$$\phi^t_{k,j} = \frac{\min_k |a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|}{|a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|} \tag{2}$$

where $a^t_{k,j}$ is the value of a observed metric j for a given node k at time t, ρ is a distinguishing coefficient normally set to 0.5, g and b are respectively the 'good' and 'bad' reference metric sequences from $\{a^t_{k,j}, k = 1, 2 \ldots K\}$, e.g. $g_j = \max_k(a^t_{k,j})$, $b_j = \min_k(a^t_{k,j})$ (where each metric is selected to be monotonically increasingly positive for trust assessment, eg Throughput). θ and ϕ are then scaled to $[0, 1]$ using the mapping $y = 1.5x - 0.5$. The vector natures of $[\theta, \phi]$ allow per-metric weighting before generating a single trust assessment, and also allows the identification and classification of untrustworthy agents. These weighted $[\theta, \phi]$ values are then condensed into a single trust value by

$$T^t_k = \frac{1}{1 + \frac{(\phi^t_k)^2}{(\theta^t_k)^2}} \tag{3}$$

For applications involving low fidelity, temporally sparse metrics with unknown statistical distributions, GRA is a more stable comparative analysis, providing an interval of potential trust values rather than fuzzy-logic or the Bayesian-Beta distributions found in current TMFs [Liu, 2006].

GRA, combined with a fuzzy whiteization model (4), and a topology-aware weighting scheme (5) provide capability to both detect the existence of a malicious agent within the network, and to classify what trust metrics that attacker is manipulating, identifying the style of attack taking place.

There are three classes of topological trust relationship; Direct, Recommendation, and Indirect. To take the example of a node n_i monitoring the trust of another, target, node, n_j; the Direct relationship is simply the trust assessment based on n_i's own observations and experience of n_j's behaviour. In the Recommendation case, another node, n_k, which shares direct relationships with both n_i and n_j, gives it's opinion on the trustworthiness of n_j to n_i. The Indirect case is similar to the recommendation case, except that the recommender n_k, does not have a (current) direct link with the target n_j but that has a direct link with the observer node, n_i.

These relationships give us node sets, N_R and N_I containing the nodes that have recommendation or indirect, relationships to the observing node respectively.

$$\begin{aligned} f_1(x) &= -x + 1 \\ f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\ f_3(x) &= x \end{aligned} \tag{4}$$

$$\begin{aligned} T_{i,j}^{net} =& \frac{1}{2} \cdot \max_s \{f_s(T_{i,j})\} T_{i,j} && \text{Direct Trust} \\ &+ \frac{|N_R|}{2|N_R| + |N_I|} \sum_{n \in N_R} \max_s \{f_s(T_{i,n})\} T_{i,n} && \text{Recommendation Trust} \\ &+ \frac{|N_I|}{2|N_R| + |N_I|} \sum_{n \in N_I} \max_s \{f_s(T_{i,n})\} T_{i,n} && \text{Indirect Trust} \end{aligned} \quad (5)$$

[Guo et al., 2011] demonstrated the stochastic variation of this methodology wrt. attack method, enabling the detection and identification of the aspect of network operation under attack. It is this work that is being expanded upon in paper.

2.4 Scenarios

Four Mobility scenarios were used in [Guo et al., 2011] to explore the trust-behaviour, covering the majority of MANET operational requirements;

- All Nodes Static
- Central node performing a random walk with leaf-nodes static
- Leaf-nodes randomly walking with central node static
- All nodes randomly walking

The six nodes were arranged in the form of a flattened pentagon with the 'central' node (n_1) placed near the geometric middle, such that each node was on average 100m from its neighbours.

In all of the scenarios, each link from $n_i \rightarrow n_j$ sent a 10 second of Constant Bit Rate (CBR) style traffic.

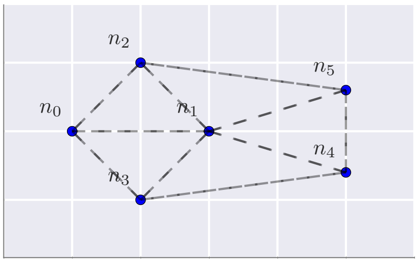

Fig. 1. Initial Scenario Topology, with nodes spaced an average of 100m apart

3 Marine Acoustic Networks

The key challenges of underwater acoustic communications are centred around the impact of slow and differential propagation of energy (RF, Optical, Acoustic) through water, and it's interfaces with the seabed / air. The resultant challenges include; long delays due to propagation, significant inter-symbol interference and Doppler spreading, fast and slow fading due to environmental effects (aquatic flora/fauna; surface weather), carrier-frequency dependent signal attenuation, multipath caused by the medium interfaces at the surface and seabed, variations in propagation speed due to depth dependant effects (salinity, temperature, pressure, gaseous concentrations and bubbling), and subsequent refractive spreading and lensing due to that same propagation variation.[Partan et al., 2006]

The attenuation that occurs in an underwater acoustic channel over a distance d for a signal about frequency f in linear and dB forms respectively is given by

$$A(d, f) = A_0 d^k a(f)^d \tag{6}$$

$$10 \log A(d, f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \tag{7}$$

where A_0 is a unit-normalising constant, k is a spreading factor (commonly taken as 1.5), and $a(f)$ is the absorption coefficient, expressed empirically using Thorp's formula (8) from [Stojanovic, 2007]

$$10 \log a(f) = 0.11 \cdot \frac{f^2}{1 + f^2} + 44 \cdot \frac{f^2}{4100 + f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \tag{8}$$

Thus, the multi-path channel transfer function can be described by

$$H(d, f) = \sum_{p=0}^{P-1} h(p) = \sum_{p=0}^{P-1} \mathit{\Gamma}_p / \sqrt{A(d_p, f)} e^{-j2\pi f \tau_p} \tag{9}$$

where $d = d_0$ is the minimal path length between the transmitter and receiver, $d_p, p = \{1, \dots P-1\}$ are the secondary path lengths, $\mathit{\Gamma}_p$ models additional losses incurred on each path such as reflection losses at the surface interface, and $\tau_p = d_p/c$ is the delay time ($c = 1500ms^{-1}$ is the nominal speed of sound underwater).

This combination of refractive lensing and the multipath nature of the medium result in supposedly "line of sight" propagation being extremely unreliable for estimating distances to targets, as the first arriving beam has as the very least bent in the medium, and commonly has bounced between the surface/seabed before arriving at a receiver. Further, this affect is usually anisotropic with differential depths between transmitter and receiver, meaning that any variation in depth across a channel, greatly impacts the characteristics of that channel.

Comparing (6) with the RF Free-Space Path Loss model (10), while both are frequency and distance dependant;

$$A_{rf}(d,f) \approx \left(\frac{4\pi f}{c}\right)^2 \text{ where } c \approx 3 \times 10^8 m/s \tag{10}$$

3.1 Trust Requirement in Marine Networks

In this subsection we establish the requirement for communications trust in acoustic marine networks, extending and expanding on the generic assessment given in 2.1

4 Initial System Model Characterisation

4.1 Simulation Background

Simulations were conducted using a Python based agent simulation framework based on SimPy[Müller and Vignaux, 2003], with a network stack built upon the AUVNetSim stack[Miquel and Montana, 2008], with transmission parameters taken from and validated against [Stojanovic, 2007] and [Stefanov and Stojanovic, 2011].

Given the differences in delay and propagation between RF and marine networks, it is natural that the same application rates (e.g. packet emission rates or throughput) cannot be maintained under such different constraints. Therefore, before we can fairly assess the trust operation of a Underwater MANET, we first establish it's operational characteristics.

Specifically, we sought to define a methodology for establishing a near-optimal operation point. This was done in two parts; optimisation for network level queuing, optimisation for physical layout scaling.

4.2 Establishing Scale Factors in Communications Rate

In this section we characterise the simulated communications environment, establishing an optimal packet emission rate for comparison against [Guo et al., 2011].

In order to establish this 'saturation point', a range of packet emission rates were explored between 0.01 packets per second (pps), equivalent to 96 bps, up to 0.07 pps (672 bps)

From 2 and 3, it is clear that the threshold curve, expressed as the *Successfully Received Packets* line, exhibits a saturation point between 0.025 and 0.03 bps. Particularly in 3, the precipitous drop in packet delivery probability beyond 0.025 pps, indicating that this would be a safe operational zone.

4.3 Establishing Scale Factors in Physical Distribution

In this section we characterise the simulated communications environment, establishing an optimal node-separation scaling for comparison against [Guo et al., 2011]

This is pretty much summarised in and 5 Varying average node separation shows that while direct throughput isn't significantly affected until, collision rates are 4. However, this collision rate is well within the tolerances of the MAC layer, as shown in 5.

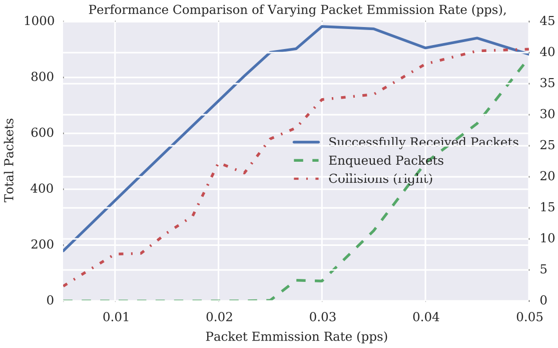

Fig. 2. Varying packet emission rate demonstrates maximal throughput at 0.025 packets per second, equivalent to ≈240 bps

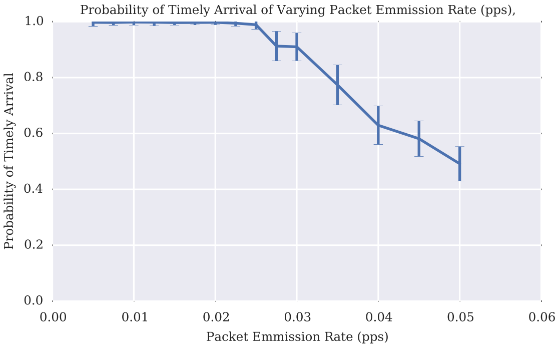

Fig. 3. Varying packet emission rate demonstrates a saturation point at 0.025 packets per second

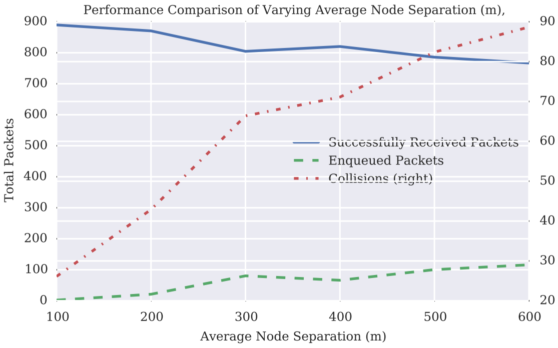

Fig. 4. Comparison of Medium Access Collisions, Throughput, and Enqueued packets against varying application packet emission rates. Scaling ratio of 3 indicated that the average distance between nodes has been tripled.

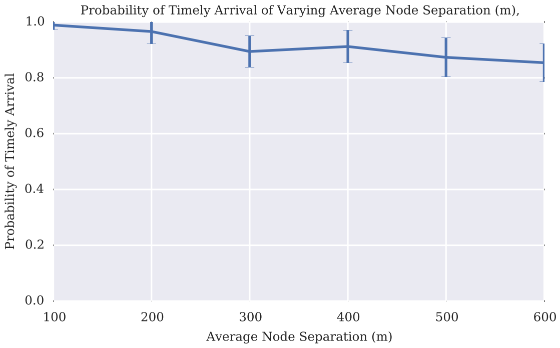

Fig. 5. Graph of probability of timely reception across a range of node scaling.

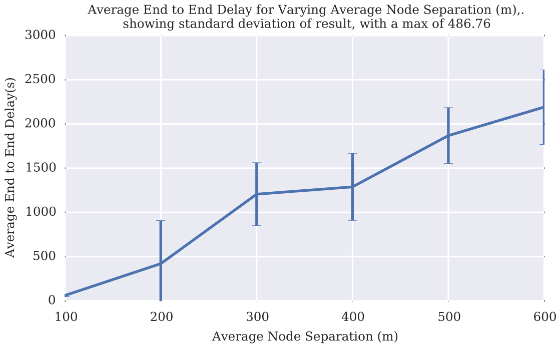

Fig. 6. Varying average node separation shows that while direct throughput isn't affected, collision rates are. However, this collision rate is well within the tolerances of the MAC layer

Acknowledgments. The heading should be treated as a subsubsection heading and should not be assigned a number.

5 The References Section

References

[Buchegger and Le Boudec, 2002] Buchegger, S. and Le Boudec, J.-Y. (2002). Performance analysis of the CONFIDANT protocol. *Proc. 3rd ACM Int. Symp. Mob. ad hoc Netw. Comput. - MobiHoc '02*, pages 226–236.

[Caiti, 2011] Caiti, A. (2011). Cooperative distributed behaviours of an AUV network for asset protection with communication constraints. *Ocean. 2011 IEEE-Spain.*

[Cho et al., 2011] Cho, J.-h., Swami, A., and Chen, I.-r. (2011). A survey on trust management for mobile ad hoc networks. *Commun. Surv. &amp; Tutorials*, 13(4):562–583.

[Guo, 2012] Guo, J. (2012). Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks.

[Guo et al., 2011] Guo, J., Marshall, A., and Zhou, B. (2011). A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad Hoc Networks. *2011IEEE 10th Int. Conf. Trust Secur. Priv. Comput. Commun.*, pages 142–149.

[Huang et al., 2010] Huang, D., Hong, X., and Gerla, M. (2010). Situation-aware trust architecture for vehicular networks. *Commun. Mag. IEEE*, (November):128–135.

[Lee and See, 2004] Lee, J. D. and See, K. A. (2004). Trust in automation: designing for appropriate reliance. *Hum. Factors*, 46(1):50–80.

[Li and Singhal, 2007] Li, H. and Singhal, M. (2007). Trust Management in Distributed Systems. *Computer (Long. Beach. Calif).*, 40(2):45–53.

[Li et al., 2007] Li, J., Li, R., Kato, J., Li, J., Liu, P., and Chen, H.-H. (2007). Future Trust Management Framework for Mobile Ad Hoc Networks. *IEEE Commun. Mag.*, 46(4):108–114.

[Liu, 2006] Liu, K. J. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE J. Sel. Areas Commun.*, 24(2):305–317.

[Miquel and Montana, 2008] Miquel, J. and Montana, J. (2008). AUVNetSim: A Simulator for Underwater Acoustic Networks. *Program*, pages 1–13.

[Moe et al., 2008] Moe, M. E. G., Helvik, B. E., and Knapskog, S. J. (2008). TSR: Trust-based secure MANET routing using HMMs. *. . . Symp. QoS Secur. . . .*, pages 83–90.

[Müller and Vignaux, 2003] Müller, K. and Vignaux, T. (2003). SimPy: Simulating Systems in Python. *ONLamp.com Python DevCenter.*

[Partan et al., 2006] Partan, J., Kurose, J., and Levine, B. N. (2006). A survey of practical issues in underwater networks. *Proc. 1st ACM Int. Work. Underw. networks WUWNet 06*, 11(4):17.

[Stefanov and Stojanovic, 2011] Stefanov, A. and Stojanovic, M. (2011). Design and performance analysis of underwater acoustic networks. *IEEE J. Sel. Areas Commun.*, 29(10):2012–2021.

[Stojanovic, 2007] Stojanovic, M. (2007). On the relationship between capacity and distance in an underwater acoustic communication channel.

[Zuo, 1995] Zuo, F. (1995). Determining Method for Grey Relational Distinguished Coefficient. *SIGICE Bull.*, 20(3):22–28.

Table 1. Comparison of system model constraints as applied between Terrestrial and Marine communications

Parameter	Unit	Terrestrial	Marine
Simulated Duration	s	300	36000
Simulated Area	km^2	0.7	0.7
Transmission Range	km	0.25	1.5
Number of Nodes		6	6
Comms Medium		RF(802.11)	Acoustic
Propagation Speed	m/s	3×10^8	1490
Center Frequency	Hz	2.6×10^9	10^3
Bandwidth	Hz	22×10^6	10^3
MAC Type		CSMA/CA	CSMA/CA
Routing Protocol		DSDV	FBR
Mobility		Various	Various
Max Speed	ms^{-1}	5	1.25
Data Rate	bps	10^6	240
Burst Counts		10	1
Packet Size	bits	4096	9600
Destination Selection		Random	Random
Single Transmission Duration	s	10	32
Single Transmission Size	bits	10^7	9600