Conference contribution :
Al-Shehri, S., Loskot, P., Numanoglu, T. & Mert, M. (2017). *Comparing tactical and commercial MANETs design strategies and performance evaluations.* Military Communications Conference (MILCOM), MILCOM 2017 - 2017 IEEE, (pp. 599-604). Baltimore, MD, USA: Proc. Military Communications Conference (MILCOM'17), 23-25 October 2017.
http://dx.doi.org/10.1109/MILCOM.2017.8170804

Comparing Tactical and Commercial MANETs

Design Strategies and Performance Evaluations

Salman M. Al-Shehri and Pavel Loskot
College of Engineering
Swansea University
Swansea, United Kingdom
{p.loskot,609122}@swan.ac.uk

Tolga Numanoğlu and Mehmet Mert
ASELSAN A.S.
Communications and IT Division
Ankara, Turkey
{tnumanoglu,mmert}@aselsan.com.tr

Abstract— **Mobile tactical networks (MTNs) in military communications extend the capabilities of mobile ad-hoc networks (MANETs). The MTNs are dynamic, infrastructure-less, self-forming and self-healing systems designed for non-line-of-sight (NLOS) operations using multi-hop relaying. Unlike their commercial counterparts, MTNs have to offer much higher levels of security, jamming resistance, and service robustness in the adverse propagation environments without sacrificing or limiting data rate, latency, and node mobility while also controlling the network capital and operational costs. Comprehensive comparison of the performance and design characteristics of the commercial MANETs and their military counterparts is carried out using NS2 simulations. It is found that, for scenarios requiring long-range connectivity, a reference point group mobility (RPGM) model and a two-way ground radio propagation model give the most accurate performance predictions for MTNs. Finally, it is argued that many commercial off-the-shelf (COTS) technologies can be adopted for their use in MTNs, even though it requires a lot of additional efforts to overcome challenges not considered by the commercial solutions.**

I. Introduction

Most commercial (i.e., non-tactical or non-military) MANET designs assume either 802.11 or short-range communications standards. However, the commercial use of large-scale MANETs appears to be non-existent. One reason is much easier deployment and management of systems with the dedicated infrastructure such as in cellular networks [1]. Moreover, in some scenarios (e.g., natural disasters and rescue operations), the supporting infrastructure may be completely disrupted. On the other hand, the MANETs are used extensively in military operations. These MANETs are enhanced by self-forming multi-hop capabilities to improve their flexibility and coverage, and to cope with a number of specific challenges in geographical areas where a well-maintained and reliable supporting infrastructure is non-existent. The architectures of MTNs are evolving towards supporting many different types of the users with heterogeneous communications and computing requirements such as in the current Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems [2]. The users are represented by sensors, surveillance satellites, unmanned aerial vehicles (UAVs), airborne platforms, various vehicles, and ground troops. The MTNs are typically operated with a restricted bandwidth in the very high and ultra-high frequency bands (UHF and VHF) which offers better network connectivity than WiFi based MANETs operated at 2.4 or 5.8 GHz [3]. Due to the nature of military operations such as tactical planning, the mobility patterns experienced in MTNs are distinctively different from those observed in other MANETs [4]. The security considerations in MTNs are paramount not only to their function, but also to the integrity and survival of the supported physical systems [6]. In order to manage the development and manufacturing costs of MTNs, the COTS technologies attracted significant interest recently. Various COTS products have been already incorporated into the military systems for a number of years such as satellites, smart devices and sensors which are adapted to various degrees to handle the harsh environmental conditions in the military scenarios [5].

The aim of this paper is to study differences between the military and commercial applications of MANETs including the requirements for communications services, network topology, and the performance metrics. Our study focuses on the deployment and operation of MTNs at the tactical edge of the battlefield theatre. A corresponding framework is created to support decisions on what technologies and solutions should be included in the future generations of MTNs.

The contents of next sections are as follows. The effective adoption of commercial information and communication technologies (ICT) at the tactical edge of the battlefield is discussed in Section II. In Section III, the main characteristics of MTNs such as the security are investigated. The properties of physical radio links in MTNs are examined in Section IV including realistic modeling of the nodes mobility and the radio propagation conditions. Conclusions are given in Section V.

II. COTS Radios for MANETs and MTNs

The recent advances in ICT also strongly impact the design of MTNs, especially at the tactical edge. The ICT reduce the time to deployment, provide advanced capabilities and reduce the operational costs of MTNs. The COTS products provide new opportunities for their use in the military domain which did not exist previously [6].

We can consider at least two perspectives to compare COTS based MANETs and their military counterparts. From the technology perspective, the COTS solutions which may be useful in tactical scenarios are cognitive radio (CR) networks, software defined radio (SDR) networks, and autonomous networks [7]. Many tactical networks rely extensively on the existing public protocols particularly at the network and transport layers [8,9], and they use the Internet protocol (IP) including its IPV6 version for traffic backhaul [10,11]. The Global Information Grid (GIG) is the main infrastructure and enterprise solution for tactical communications developed by the Department of Defence (DOD). It comprises a mixture of many proprietary military and public COTS technologies. However, majority of the military users consider the use of public COTS technologies to present severe security threats, since the 3rd parties may have accurate knowledge of the functioning and structure of some internal components and subsystems. Using the COTS security solutions in MTNs is often challenging or even undesirable [12].

From the economical perspective, the economies of scale are vital for offering affordable commercial products. This is more difficult to achieve for the military products, even though the demands for the cyber-security solutions, navigation systems and UAVs have increased considerably in the recent years. The defence manufacturers are now focusing on advancing the lightweight electronics, small antennas, and other radio frequency (RF) technologies [13]. The COTS hardware and software is finding its way to the Internet of Things (IoT) in the military C4ISR structures [14]. Since the level of financial support determines the achievable capabilities and performance of the technology, it is likely that the commercial drivers will influence the future developments of the military networks much more than ever before.

A. *Technology challenges at the tactical edge*

The conditions encountered by MTNs are vastly different from those assumed in the deployment and operation of commercial ICT products. Hence, the military sector has a long history of developing bespoke technological solutions. The cost benefits of COTS solutions together with careful planning create new opportunities to use these technologies in military applications. However, the cheap solutions may entail the security and robustness concerns [15]. One has to also consider typical radio communication trade-offs between the capacity, range and data rates. In order to serve much higher demands for data rates, the newer MTNs are primarily using larger bandwidths between 4.4 to 5.4 GHz under more line-of-sight (LOS) conditions whereas the legacy MTNs were designed for the 1350-2690 MHz frequency bands and NLOS transmissions. Overall, the challenges in using COTS solutions in military communications can be summarized as follows [16,17]:

1) Insufficient support for mobility to the degree encountered in many MTNs.

2) The commercial pressures for short development cycles leading to frequent technology updates is rather undesirable in military applications.

3) The market dynamics for military products and the resulting returns on investment (ROI) are very different from those in the commercial sector.

4) The commercial vendors of ICT equipment do not have sufficient experience or capabilities to deliver military grade products, for example, to guarantee the quality of service (QoS) over wide range of operating and often quite adverse conditions.

5) The cost efficiency of COTS solutions may be completely offset by the lack of reliability and performance guarantees in the realistic military environments.

B. *Unique technological requirements*

The barriers to adoption of commercial ICT in the military context primarily arise due to unique requirements at the tactical edge and involve the policy, environmental and technical considerations including, but not limited to, the robustness of services provisioning and the information assurance. In addition, MTNs have significantly stringent security requirements than the commercial MANETs. Therefore, a direct adoption of COTS technologies without adjustment is not recommended [18]. In some applications, the constraints of the original COTS design can be accepted [24]. For example, the commercial-grade radios can operate successfully provided that the mobility of nodes in MTNs is limited, even though the full spectrum management may be problematic [19]. It is useful to recognize that the latest, function-rich COTS technologies may be less suitable for use in military systems, and that their adoption may still require significant purpose-driven research and further development.

III. MAIN CHARACTERISTICS OF MTNS

There are different types of MTNs designed for different applications and scenarios. These MTNs differ in their requirements for data rates, latency, and transmission ranges, and they involve nodes with the small hand-held or vehicle-mounted transceivers. Here, our focus is mainly on the long-range MTNs with the limited bandwidth to compare their performance with the commercial MANETs. In this section, we discuss crucial differences between these two kinds of networks, and point out which differences are not easy to overcome.

A. *Protocols for multi-hop networks*

In mission-critical networks, the mobile nodes must communicate with the minimum disruptions and delays. This requires efficient and robust routing protocols. The conventional cellular networks were designed to utilize one-hop connections, and they operate in very predictable environments and traffic conditions. These assumptions are rarely satisfied in the deployment of MANETs. Several protocols for MANETs with multi-hop capabilities were adopted for MTNs [20]. However, these proposals usually consider the Wi-Fi connectivity for the protocol testing and evaluations which is inadequate for the VHF/UHF connectivity in MTNs [21]. In addition, the protocols used in MANETs mostly assume that these networks are very homogeneous (i.e., the nodes have the same communication and processing capabilities) which is rarely if ever satisfied in MTNs [22]. The MTNs are highly heterogeneous with hierarchical network topology and the different types of radio equipment and functional interfaces having different communications and computing constraints. The routing in MTNs is done hierarchically at the local and global level with a backup option to switch to a flat-topology routing. Furthermore, most traffic in MANETs is point-to-point whereas significant portion of traffic in MTNs is multicast and broadcast for group-oriented communications [23].

At the transport layer, the connection-less UDP protocol is a preferred choice for MTNs. It requires that the application layer protocol guarantees the information delivery. The Stream Control Transmission Protocol (SCTP) has been developed as an effective alternative to TCP and UDP for provisioning of the WWW (Word Wide Web) services in MTNs [18]. The Media Access Control (MAC) protocols must be selected for the VHF/UHF propagation conditions [24]. Both Carrier Sense Multiple Access (CSMA) protocols [25] and Time Division Multiple Access (TDMA) protocols [26] were considered for MTNs. The latter protocol provides a collision-free delivery, and can improve the performance of MTNs under the severe environmental and resource constraints. In summary, and more importantly, the protocols for MTNs must be tested for highly dynamic topology changes under connectivity characteristics observed in the realistic terrains and environments.

B. *Security issues in MTNs*

The MTNs are operated in the hostile environments, so their security must be embedded in their design from the inception [27]. The security threats are more severe when the proprietary networks are open to external access, e.g. via the Internet. The provisioning of security in MTNs is also more challenging due to the nodes mobility, a need for high data rates over larger bandwidths, and the wireless broadcast. The distributed nature of wireless protocols makes these networks more prone to jamming and eavesdropping [28]. In addition, the security attacks are constantly evolving and becoming more sophisticated. The security risks and protection mechanisms in commercial MANETs are relatively well understood, unlike the security of MTNs which is comparatively unexplored in the open literature. The main threats to MTNs are cyber-attacks, cyber espionage, physical attacks and inadequate information control mechanisms. The cyber-attacks involve both passive methods (e.g., traffic analysis), and active methods (e.g., packets replay) [38]. Recently, the cyber-security in military communication networks has merged within the electronic warfare, resulting in so-called information warfare. In general, the aim of the electronic warfare is to gain control of the electromagnetic spectrum [29] by:

- the electronic attacks and the use of electromagnetic energy to degrade the communications services;
- the electronics protection of equipment and of electromagnetic spectrum to prevent degradation or damage of the communication capabilities; and
- the actions taken to locate and prevent the intentional and unintentional electromagnetic radiations.

IV. PEFORMANCE COMPARISON

The performance of MTN architectures is evaluated by simulations using NS2 software. In practice, the field-tests are mandatory to gain trust and confidence in the designed MTNs, even though these tests are time-consuming, costly, and they may not be up to scale.

A. *Performance metrics*

The choice of appropriate performance metrics is important for effective design process. Here, we assume the following network metrics:

- the packet delivery ratio (PDR) is a fraction of the successfully delivered packets;
- the routing overhead is the amount of control data required to make the routing decisions;
- the average throughput is the average number of the successfully delivered bits in a unit of time; and
- the end-to-end delay is the time required for the packet to be fully received at the destination.

B. *Network deployment scenario*

The current MTNs involve between 20 to 60 nodes which may scale up to 200 nodes in the future designs. The MTNs usually operate in the field of size, say, 10 by 10 km. The nodes are divided into several groups, and each group has its group leader. One of the group leaders also serves as the main leader of all the other groups. The nodes are uniformly distributed about their group leaders who are following the main leader by maintaining a constant distance and the same direction. This yields a mobility pattern that is best described by the RPGM model [30]. The nodes travel at speeds 30-80 km/h, and the mobility is interleaved with pauses of up to 30 min in duration.

C. *Numerical examples*

We assume the realistic mobility and radio propagation models, as well as the multi-hop capabilities of MTNs. The simulation parameters are summarized in Table I.

TABLE I. SIMULATION PARAMETERS

Object	Parameter	Value
Network node	Medium	Wireless channel
	RF propagation	Free space, and two-ray ground models
	MAC	802.11
	Antenna	Omni-directional
	Routing protocol	AODV-HAODV
	Number of nodes	25-250
	Packet size	512 bytes
	Mobility	RWP, RPGM, Manhattan
Network scenario	Simulation time	1000 sec
	Simulation area	10 km × 10 km
	Pause time	30 sec
	Speed	80 km/h
	Transmit power	46 dBm for vehicles and 30 dBm for patrols

Effect of mobility models

The mobility models have large impact on the performance of MANETs, since the mobility affects the length of the routing path, the path stability, and the number of neighbors of the nodes [31]. We assume the following 3 mobility models: random waypoint (RWP) model, RPGM, Manhattan mobility model, freeway mobility model, and the Gauss-Markov mobility model [32]. Importantly, in military scenarios, the node movements are influenced by the headquarters or by the mission commander as well as by the tactical goals of the mission. The nodes in MTNs need to closely collaborate, so their movements are highly correlated. It leads to formation of the mobility groups which are following the mission leader. In such scenarios where the swarming phenomenon occurs, the RPGM model best describes the node movements. In contrast, the MANET nodes in commercial applications usually moves in less coordinated way, so the random mobility models are more appropriate in these situations.

Next, we numerically compare the responses of commercial MANETs and MTNs assuming different mobility models. All simulation results were obtained in the NS2 software. The packet delivery ratio (rate) values for commercial MANETs and MTNs are shown Fig. 1. The varying number of nodes in the network represents different traffic loads. We observe that the RPGM model yields the best performance, and it outperforms the other two mobility models considered by 75% on average while the RPGM describes the mobility in MTNs more accurately. The average throughput and the average delay for the same set of experiments are then shown in Fig. 2 and Fig. 3, respectively. We can again observe that other mobility models underestimate the performance of MTNs compared to the performance of the more realistic RPGM model. This behavior appears to hold for any traffic loads in the network.

The performance bias of different mobility models is also observed when considering the routing overheads as shown in Fig. 4. In particular, for 25 nodes, the RPGM model has the overhead ratio at least 1.3 times better than the other two models, and it reaches the largest improvement for 50 network nodes, resulting in the overhead ratio decrease by 143.

Effect of radio propagation models

Another key factor significantly affecting the performance is the choice of radio propagation models. Provided that we assume a radio propagation model that does not accurately describe the realistic propagation conditions, it can substantially either underestimate or overestimate the system performance. The two most important parameters to consider in the radio propagation models are the carrier frequency and the transmission distances between the transmitting and receiving antennas. More specifically, we compare the network performance for the two propagation models: a free-space path loss model and a two-ray model [33]. For mobility, we assume the RPGM model in all simulations.

The packet delivery ratio is shown in Fig. 5. We observe that, for any network load, the two-ray propagation model always outperforms the free space model by about 13%. The former model is better aligned with the NLOS propagation conditions in the realistic deployments that the MTNs usually experience. Interestingly, the obstacles within the environment which create the NLOS conditions may reduce the co-channel interference, and actually improve the system performance. Thus, should the free space model be used for simulations of MTNs, it would underestimate the real performance. On the other hand, the commercial MANETs are often designed and operated in more line-of-sight conditions (e.g., small, battery powered sensor nodes), so assuming the free space model to evaluate the performance of these networks can be justified.

Fig. 6 compares the average throughput and Fig. 7 shows the average delay results for the two propagation models considered. We observe that, on average, the two-ray propagation model always outperforms the free space model by about 167 bits/sec in terms of the average throughput, and by about 150 msec in term of the average delay.

Finally, Fig. 8 compares the routing overhead under the same conditions as in Fig. 6 and Fig. 7. On average, the two-ray model outperforms the free-space model by providing at least 0.5 smaller routing overhead.

D. Discussion

The NS2 simulation environment was chosen as it is freely available, relatively fast even for networks containing 100's of nodes, and especially due to its support of the wireless networking protocols including wireless sensor networks (WSNs) and MANETs, and the support of various mobility models and the propagation environments.

As observed in the previous sub-section, the choice of propagation models has significant impact on the observed performance in simulations. This in turn affects the technology decisions when designing these networks. The most effective way of obtaining accurate physical models including the node mobility and radio propagation models is to use measurements from the real networks. However, this can be problematic when dealing with proprietary network, or when the measurements would disclose the commercially sensitive performance characteristics of the network products. Even when this is not the case, the collected measurements may be very specific to the environment and the deployment conditions, so drawing any general conclusions may not be meaningful.

Another strategy is to assume multiple models covering different scenarios and operating environments. If the performance for one or more of these models is not acceptable, the designers must decide whether the considered models are relevant, or whether they can be excluded from further investigations. It is also common to use the designed networks for the applications other than the ones for which they were developed. In these situations, the network protocols can be modified, new control and networking modules can be added, or different types of antennas may be considered. Such a case occurs when the MANETs built with the COTS components are used as MTNs with the military applications.

Alternatively, the use of hardware testbeds for research and development is becoming attractive. Their main advantage is the speed of obtaining the performance results in spite of using more complex, and thus, possibly also more realistic models. However, the hardware testbeds limit the maximum size of the network under consideration, and the initial capital investments can be quite high unless it can be shared by several research labs. One of the main drivers of the NS3 as a successor of the NS2 software is to provide a native support for the testbeds.

V. Conclusions

When considering the implementations of MANETs in the tactical space for military applications, it is essential to consider the type of transceivers and communication platforms deployed, in addition to application requirements. The unique attributes of MTNs including the specific environment characteristics and deployment scenarios as discussed in this paper have a significant impact on the adoption of MANETs for military use. Thus, assuming generic MANET solutions for the use in military applications can be very misleading in achieving the trustable and reliable military grade MTNs.

Despite a vast progress in commercial technologies including ICT, the COTS solutions cannot be used directly, but have to be adapted to the military needs by continuing and focused research efforts. The research and development towards enhanced capabilities of MTNs is only as good as the accuracy of the underlying physical models considered in their design, especially concerning the mobility and radio propagation models. The MTNs are more demanding and use (often proprietary) protocols to support multi-hop self-forming and self-healing features. Moreover, it is critical to consider the security threats which are often of different nature than in the public cyber networks. As the ICT are getting more complex while also becoming the critical part of the communications and physical infrastructures, the use of hardware and software COTS solutions poses severe security risks. The security testing of complex hardware and software components from the 3rd party developers and suppliers is an open and challenging research problem.

Our numerical results confirm the importance of choosing the right models to evaluate the performance of MTNs in order to capture the realistic dynamics of the military networks. We argued that the RGPM model for node mobility and the two-ray model for radio propagation are the most realistic choices to describe the deployment and operation of MTNs. Our simulations provide critical insights into the characteristics of typical MTNs. We found that both these models yield much better performance of MTNs than other models which appear to underestimate their performances. Such characteristics were generally observed for all the performance metrics considered. However, the most appropriate physical models for deploying MANETs in non-military or civilian applications are likely to be different. Such considerations are imperative when adopting general purpose MANETs for their use as MTNs.

In summary, the general purpose MANETs built with COTS technologies are applicable to MTNs, however, one has to consider very different radio propagation and mobility models as well as complex security issues due to the untrusted 3rd party suppliers of hardware and software components.

References

[1] C. E. Fossa and T. G. Macdonald, "Internetworking tactical MANETs," In *MILCOM*, 2010, pp. 611-616.

[2] N. R. Council, D. E. P. Sciences, N. S. Board, and C. C. F. N. S. Groups, *C4ISR for Future Naval Strike Groups*. National Academies Press, 2006.

[3] H. Wang et al., "Implementing Mobile Ad Hoc Networking over Legacy Tactical Radio Links," In *MILCOM,* 2007, pp. 1-7.

[4] Y. Zhang et al., "Data replication in mobile tactical net.," In *MILCOM*, 2011, pp. 797-803.

[5] B. Thompson and R. Harang, "Identifying key cyber-physical terrain," In *IWSPA,* 2017, pp. 1-16.

[6] M. Tortonesi et al., "Enabling the deployment of COTS applications in tactical edge networks," *IEEE Commun. Mag.,* vol. 51, pp. 66-73, 2013.

[7] J. R. Agre, K. D. Gordon, and M. S. Vassiliou, "Commercial Technology at the Tactical Edge," 2013. Available: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA587552

[8] J. R. Agre;, K. D. Gordon;, and M. S. Vassiliou, "C2 in Underdeveloped, Degraded and Denied Operational Environments," 2013.

[9] E. Larsen, "TCP in MANETs – challenges and solutions," Norwegian Defence Research Establishment (FFI) 2012.

[10] A. Morelli, R. Kohler, C. Stefanelli, N. Suri, and M. Tortonesi, "Supporting COTS applications in tactical edge networks," In *MILCOM*, 2012, pp. 1-7.

[11] G. F. Elmasry, *Tactical Wireless Communications and Networks: Design Concepts and Challenges*. John Wiley & Sons, 2012.

[12] J. L. Burbank and W. T. Kasch, "Transforming legacy network systems for use in the Army Future Force," In *MILCOM,* 2004, pp. 1179-1185.

[13] R. Koch and G. D. Rodosek, "The role of COTS products for high security systems," In *CYCON*, 2012, pp. 1-14.

[14] Aerospace and Defence Market Trends, "Global C4ISR Market," 2016.

[15] N. Suri *et al*., "Analyzing the applicability of Internet of Things to the battlefield environment," In *ICMCIS*, 2016, pp. 1-8.

[16] J. L. Burbank and W. T. Kasch, "COTS communications technologies for DoD applications: challenges and limitations," In *MILCOM,* 2004, pp. 1172-1178.

[17] M. S. Vassiliou et al., "Crucial differences between commercial and military communications technology needs: Why the military still needs its own research," In *MILCOM*, 2013, pp. 342-347.

[18] S. Marsden; and J. Vankka, "Providing a tactical domain for an independenet Task Force," In *ISMS*, 2015.

[19] M. S. Vassiliou, D. S. Alberts, and J. R. Agre, *C2 Re-envisioned: The Future of the Enterprise*. CRC Press, 2014.

[20] F. Arreghini et al., "Heterogeneous network testbed for tactical communication in shore scenario," In *MILCOM*, 2015, pp. 483-488.

[21] L. Li and T. Kunz, "Efficient mobile networking for tactical radios," In *MILCOM*, 2009, pp. 1-7.

[22] H. Safa et al., "HAODV: A New Routing Protocol to Support Interoperability in Heterogeneous MANET," In *AICCSA*, 2007, pp. 893-900.

[23] N. Aschenbruck, E. Gerhards-Padilla, and P. Martini, "A survey on mobility models for performance analysis in tactical mobile networks," *J. Telecommun. Inf. Technol.,* pp. 54-61, 2008.

[24] L. Y. Cheung; and C. W. Yin, "Designing Tactical Networks – Perspectives from a Practitioner,"DSTA Horizons, June 2013.

[25] G. R. Kelsch, "A comparison of battlefield CSMA networks with theoretical network analysis," In *MILCOM*, 1999, pp. 761-765.

[26] B. Suman, L. Mangal, and S. Sharma, "Analyzing Impact of TDMA MAC Framing Structure on Network Throughput for Tactical MANET Waveforms," In *CAC2S*, 2013.

[27] J. Kerdsri and K. Wipusitwarkun, "Network virtualization for military application: review and initial development of conceptual design," In *ICACT,* 2012, pp. 61-66.

[28] S. J. Yoon and Y. B. Ko, "JRGP: Jamming resilient geocasting protocol for mobile tactical ad hoc networks," In *ICTC*, 2010, pp. 437-442.

[29] Headquarters, DoA, "Electronic Warfare in Operations," Washington D.C., 2009, Available: http://usacac.army.mil/

[30] L. Li et al., "Network properties of mobile tactical scenarios," *Wireless Commun. Mob. Comp.,* vol. 14, pp. 1420-1434, 2014.

[31] S. Rho et al., "Group Mobility Model Based on Mobility Prediction in Tactical Network On-The-Move," In *CUTE*, 2010, pp. 1-6.

[32] S. Batabyal and P. Bhaumik, "Mobility Models, Traces and Impact of Mobility on Opportunistic Routing Algorithms: A Survey," *IEEE Commun. Surveys Tutor.,* vol. 17, pp. 1679-1707, 2015.

[33] S. Reidt et al., "Resource-constrained signal propagation modeling for tactical mobile ad hoc networks," In *Net. Sci. Workshop*, 2011, pp. 67-74.

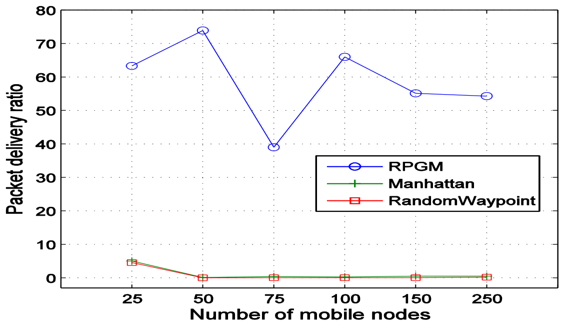

Fig. 1. The packet delivery ratio versus the number of nodes.

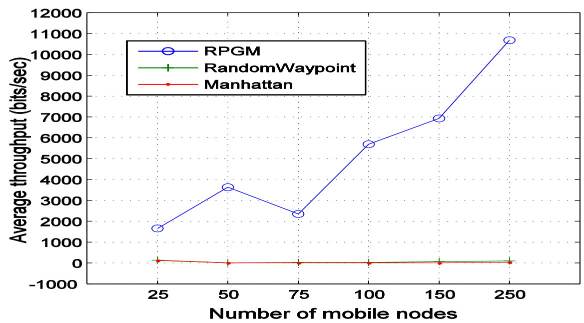

Fig. 2. The average throughput versus the number of nodes.

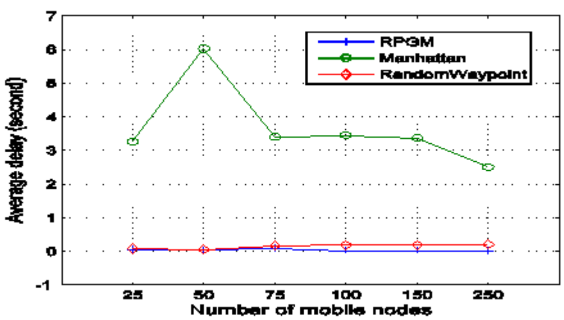

Fig. 3. The average delay versus the number of nodes.

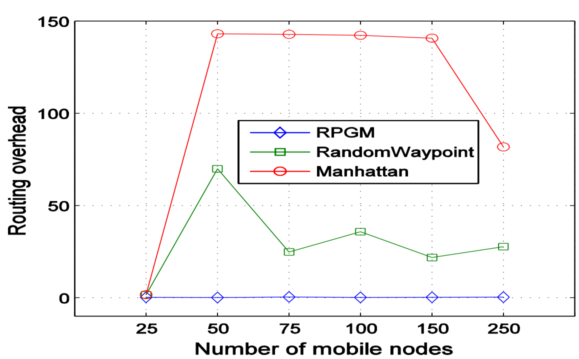

Fig. 4. The routing overhead versus the number of nodes.

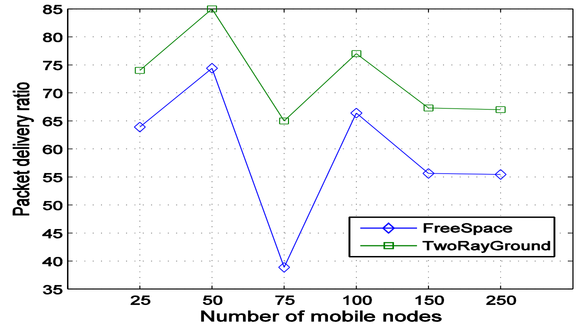

Fig. 5. The packet delivery ratio versus the number of nodes.

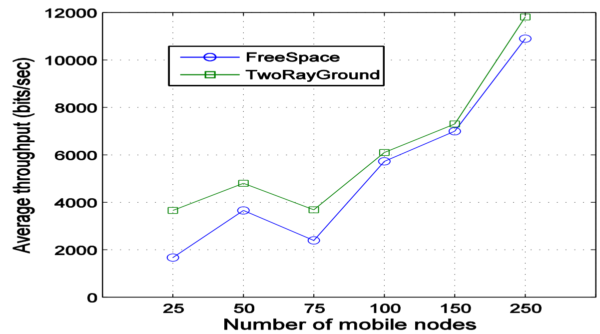

Fig. 6. The average throughput versus the number of nodes.

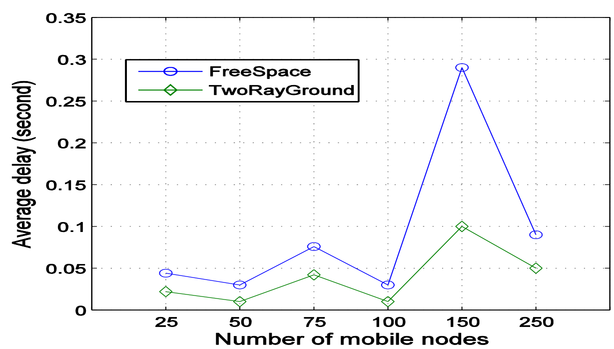

Fig. 7. The average delay versus the number of nodes.

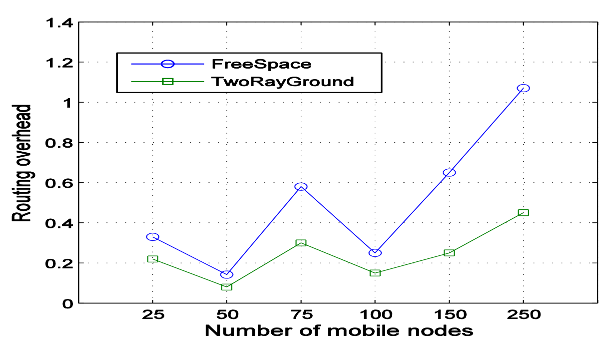

Fig. 8. The routing overhead versus the number of nodes.