Scientific Research Publishing

Wireless Sensor Network, 2016, 8, 211-228
http://www.scirp.org/journal/wsn
ISSN Online: 1945-3086
ISSN Print: 1945-3078

Dependability in Future Battle Network System
—Transport Layer Ability to Maintain Quality of Service

Veiko Dieves

Center for Applied Research, Estonian National Defence College, Tartu, Estonia
Email: veiko.dieves@mil.ee

How to cite this paper: Dieves, V. (2016) Dependability in Future Battle Network System—Transport Layer Ability to Maintain Quality of Service. *Wireless Sensor Network*, **8**, 211-228.
http://dx.doi.org/10.4236/wsn.2016.810017

Received: October 27, 2016
Accepted: October 29, 2016
Published: October 31, 2016

Abstract

Modernization of armies is a constant process and is driven by intuitive fact that those who do not modernize will become extinct. In last five decades, the development of modern armies has taken place around Colonel John Boyd's theory of OODA loop that deals with information superiority. Building a robust, mobile and capable network that could provide for novel appliances and information superiority is the main challenge which modernizers are facing. Network, suitable for future combat operations, and able to transport a vast amount of information on a battlefield, is expensive to build. Every mistake in design and the need to correct those mistakes could halt development in an army for years. Therefore, system dependability analysis during system design phase is needed. In this report, the concept of a future Battle Network System is described. The Report evaluates operational environment of BNS and possible failure reasons of the service, and illustrates the change in BNS Quality of Service due to probable transport layer errors. This paper describes the method of testing the concept of proposed network systems on the drawing board, and emphasizes design points for a new system. Nevertheless, the proposed method is by no means conclusive. Rather, it describes an engineering approach to define the main problems while creating MANET-based networking systems.

Keywords

Combat Systems Network, Battle Network System, Transport Layer, Quality of Service, Dependability Evaluation, MANET

1. Introduction

The concept of future Battle Network System has been proposed. Battle Network System (BNS), also known as Combat Systems Network [1] is described by five

layers: sensors and platforms, services, applications, transport layer and standards. Transport layer itself is described as a system consisting of eight subsystems:

1) *Tactical airborne subsystem*;
2) *Maneuvre leader subsystem*;
3) *Combat radio subsystem*;
4) *Cable network subsystem*;
5) *Mounted local subsystem*;
6) *Data distribution subsystem*;
7) *Tactical trunk subsystem*;
8) *Command-post module subsystem*.

In addition to that system, Quality of Service (QoS) benchmarks have been described. In order to evaluate if transport layer is able to reach those benchmarks, one thing has to be understood that the transport layer must maintain Quality of Service on an area of 40 × 40 km. This is a military unit's area of operations (AO) roughly equivalent to Infantry Brigade. A Brigade is the largest military unit that is still considered to operate on a tactical level. A Brigade consists of 5 different levels of subunits, all connected to BNS. As a tactical level unit, a Brigade is characterized by several features. First, AO is constantly expanding and collapsing. Second, AO is in constant move on all directions. Third, subunits of Brigade are in constant dynamic and seemingly random moving. Every subunit is equipped with one or two nodes. That means the whole Brigade has approximately 500 nodes.

Above the Brigade, there is one more level of units that have to be connected to BNS (operational level). Every subunit's level has its own set of services which it has access to. Quality of Service benchmarks have been described for every service point in three categories: time tolerance of transmission, tolerance for mistakes and data transmission speed. Table 1 describes QoS benchmarks in BNS.

The concept of Battle Network System (BNS) determines network on that area is mainly created as Mobile Ad-Hoc Network (MANET). Main subunits of BNS are maneuver leader subsystem, combat radio subsystem and tactical trunk subsystem, all of them working as a MANET. Therefore, previous analysis of MANET could be used to evaluate BNS. Tactical trunk subsystem acts as a backbone of BNS. It consists of nodes capable to form connections with each other similar node over the AO of Brigade. The concept states that nodes forming tactical trunk subsystem have to be operational within 15 min after arriving to a new position. All other subsystems connect through a gateway to tactical trunk subsystem. Combat radio subsystem is the main subsystem used by maneuver units. It consists of nodes carried by fighting vehicles, sometimes also by soldiers (signalers). Combat radio subsystem forms local MANETs that are connected with tactical trunk subsystem through a gateway to residing on company level. Maneuver leader subsystem is an extension of combat radio subsystem.

Table 1. Quality of Service benchmarks in BNS.

Services	Sub-services	QoS benchmarks		
		Delay	Mistakes allowed	Data rate
Voice	K1	<250 ms	Some	1 Mbps
	K2	<250 ms	Some	1 Mbps
	K3	<250 ms	Some	1 Mbps
Video	V1	<250 ms	Some	>1 Mbps
	V2	<250 ms	None	>1 Mbps
NCC	J1	250 ms - 10 s	None	<64 kbps
	J2	10 s - 1 min	None	1 Mbps
	J3	10 s - 1 min	None	1 Mbps
	J4	10 s - 1 min	None	1 Mbps
	J5	10 s - 1 min	None	1 Mbps
	J6	10 s - 1 min	None	1 Mbps
	J7	10 s - 1 min	None	1 Mbps
	J8	250 ms - 10 s	None	1 Mbps
	J9	250 ms - 10 s	None	1 Mbps
	J10	10 s - 1 min	None	>1 Mbps
	J11	10 s - 1 min	None	1 Mbps
	J12	250 ms - 10 s	None	1 Mbps
	J13	250 ms - 10 s	None	1 Mbps
	J14	250 ms - 10 s	None	1 Mbps
NCC	J15	250 ms - 10 s	None	1 Mbps
Security	I1	NDITT	NDITT	NDITT
	I2	NDITT	NDITT	NDITT
SCS	U1	>1 min	None	<64 kbps
	U2	>1 min	None	<64 kbps
	U3	>1 min	None	<64 kbps
	U4	10 s - 1 min	None	<64 kbps
	U5	10 s - 1 min	None	<64 kbps

NCC—Network Centric Command; SCS—Strategic Central Services; NDITT—Not Described In Those Terms.

It allows a unit commander to dismount and lead his or her subordinates while still receiving all services of BNS.

MANET is a network concept emerged from earlier mesh-network concept. It is a continuously self-configuring network of mobile devices that are connected wirelessly. MANET nodes are able to move randomly in an operational area, while still maintaining a working network. Data packets are exchanged between

different nodes using hop. Point-to-point connections between sender and receiver are not needed, though BNS concept states when low delay is needed, e.g. with voice and video subservices, BNS will try to create a point-to-point connection.

QoS in MANET is always "soft", meaning that with constantly changing environment and network architecture, it is not possible to ensure continuous service to all nodes: some of nodes will be at least some time out of service. Therefore, it is not easy to express dependability in MANET with solid number. There are other problems with MANET like path loss, multipath fading, link outage probability, node outage probability, shadowing, hidden terminal problem, exposed terminal problem, etc. Battlefield is a complex environment with many emerging problems, but due to the fact that BNS is described only on concept level, it is not feasible to analyze all aspects of dependability of the system. In this report, node outage problem, hidden terminal problem and those problems impact on QoS will be discussed.

Due to the features of existing military MANET radios, one network can consist of maximum 30 - 40 nodes. In order to merge those subnetworks together and work seamlessly, one extra node (gateway) has to be placed on subunits level. Every one of those gateways serves as a critical node for the network. The node is critical if its sudden failure divides a network into two disconnected sub networks [2]. The report will discuss critical links on a battlefield and how this fundamentally affects QoS in BNS.

Throughout recent military history (last 200 years), one certain characteristic has described developments on the battlefield, namely the spreading out of troops and fighting platforms. Spread has several advantages:

1) It is more difficult to determine the position of troops by the enemy;
2) It is more difficult to attack identified troops and cause them excessive damage by the enemy;
3) It is easier to conduct synchronous maneuver with own troops if there is maneuvering space.

The main disadvantage of spread is the weakening of communications. Spread of troops will make it harder to form point-to-point links between nodes allocated to the troops. The same is also true in BNS. The concept describes AOs for different subunits and propagation of signals. As shown in **Table 2**, on platoon level and up communication is near-line-of-sight or beyond-line-of-sight.

Those parameters should be kept in mind while evaluating QoS in BNS.

2. Dependability on a Battlefield

Dependability of systems on a battlefield has important implications. Every mistake in system design or operations could have catastrophic consequences if a necessary service is not delivered. Therefore, before analyzing dependability of the BNS, one has to understand what a battlefield is, how it is organized and

Table 2. Spread effect on LOS.

Spread effect on LOS		
Unit	*Distance*	*AO* (km²)
Brigade	BLOS	1600
Battalion	BLOS	48
Company	nLOS	8
Platoon	nLOS	5
Squad	LOS	2
Dismounted leader	LOS	0.5

AO—Area of Operations; BLOS—Beyond Line of Sight; nLOS—near Line of Sight; LOS—Line of Sight.

what are the main threats regarding the system service delivery continuity perspective.

The conventional battlefield is continuous and linear [3]. It consists of security area (forward area of a battlefield), main battle area and rear area. Security area is established in order to protect main fighting force from unexpected enemy attack. Most sensors and reconnaissance units (human sensors) are operating in security area. First, sensors are discovering and identifying enemy units passing through security area. Second, security units are conducting short firefights, therefore, forcing enemy to slow its approach towards main friendly unit and revealing its positions, maneuver and plans. Third, sensors will continue to work in enemy's rear that has already passed through security area in order to detect enemy's fire support units, second echelon, reserve and its traveling route, in order to give indications what are his plans.

On the main battle area, bulks of fighting units are operating. Those units consist of mostly infantry and armor. These are also called maneuver units or main operators. The concept of BNS is defining those units as main clients of different services. Maneuver units are more mobile than other units and QoS in MANET of those units is harder to achieve than elsewhere. Therefore, analyzing QoS in MANET should further concentrate to QoS for main operators.

On the rear area, combat support and combat service support units are operating. The *raison d'être* of those units is to support and serve the needs of main operators, e.g. fire support, engineering, air defense, logistics etc. Most services described in BNS are passing information between main operators and support units. Nodes used here are mostly vehicle mounted.

Units' concentration on a battlefield varies. Spread is greater in security area and rear area. In main battle area, concentration of forces is greater; therefore, also concentration of nodes is greater. Figure 1 described that spread difference. Dots are representing clusters of nodes forming local MANETs. As figure shows, the spread of units and nodes lessens in the second quarter (counted from the right side) of AO (represented by rectangular out-shape) and starts then to widen again.

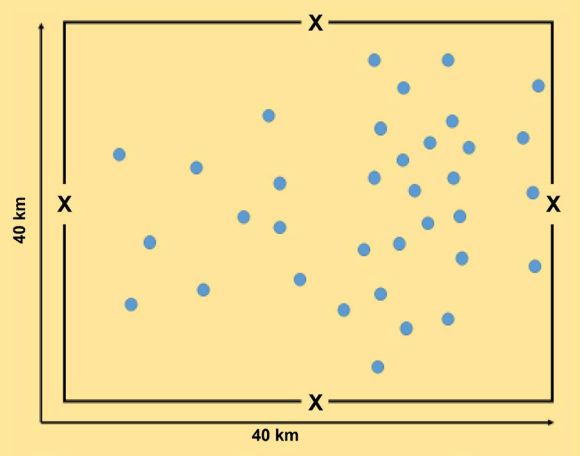

Figure 1. Spread difference of nodes.

Usually MANET architecture describes also the architecture of Internet in order to describe a gateway. That is not so with the concept of BNS. BNS will be built in a way that it is capable of working without Internet connection independently (although BNS can use some services over Internet).

NCC services described in BNS concept are providing situational awareness to the units. That part of BNS will form Battle Management System or BMS. There are several problems on a battlefield that BMS is designed to overcome. In this report, we will discuss target engagement (here in the meaning of processes taking place on tactical level before and during engagement with fire), close maneuver of different subunits and indirect fires coordination.

Target engagement and targeting are closely related. On a tactical level, those include identification, selection and prioritization of targets, combat identification, and engagement with fire and battlefield damage assessment [4]. As Joint Publication 3-09 states, "engaging forces must maintain vigilance on the location and movement of friendly forces throughout the engagement—friendly forces tracking is […] linked to combat identification […]." That means prior and during the engagement engaging force has to have a good awareness of friendly forces locations and movement. In future battlefield, friendly forces tracking subservice is meant to solve that problem by providing data of all the nodes connected to BNS locations of other nodes. Here is where hidden terminal problem will come in.

Hidden terminal is a well-known problem of MANET. It is essentially an inability to receive a signal from one node by another node because third node's is already sending a signal to the second node, while unaware of another signal being sent [5]. We could easily imagine that on a battlefield, where signal paths vary and randomly change, hidden terminal problem is constantly affecting friendly forces tracking service, and therefore, safety of own troops, especially in time critical situations. Let us picture a hypothetic situation where squad leader tries to identify friendly and enemy vehicles on a battlefield. Squad leader spots

an APC (Armored Personnel Carrier) in distance and is not sure if that happens to be friendly or non-friendly weapon platform. In order to answer that question, squad leader will check his/her BMS interface. If that actually happens to be a friendly unit whose friendly forces tracking subservice has failed to update because of hidden terminal problem, squad leader will identify it as an enemy unit and will engage it with fire. MANET problem has led to catastrophic consequences.

Maneuvering of subunits is another example where BNS dependability is critical. Closely moving and fighting subunits whose maneuvers are not coordinated by one entity and who does not share the same channel for all communications, could pose a threat to each other. Due to fog of war, friendly units could mistake each other as enemies, and engage with fire. Also, every subunit uses certain amount of space for its own purposes, namely for maneuver. Free space around a subunit allows it to plan its movement independently and does not require it to de-conflict its use of battlespace with other subunits. If battlespace has not been allocated, different subunits would collide with each other and disrupt each other maneuvers. That in return would slow down a tactical and operational tempo, leading to loss of information and tempo superiority. Eventually it would lead to losses on a battlefield. To counter this threat, at the present restrictive boundaries are placed between maneuver units AOs, separating maneuver units to operate in their distinct areas. However, this in turn also weakens the principle of concentration of forces in decisive moment. In the future battlefield, BMS should be able solve that problem by providing friendly units with Common Operating Picture or COP. COP subservice should inform own units not only about friendly locations, but also enemy locations on a battlefield. That should make possible to conduct safe close maneuvers with great operational tempo without restricting subunits to their respective AOs, concentrating forces in decisive moments and maneuvering them through the same battlespace at the same time, in different directions. Sudden QoS failure to provide COP could lead to stumble of forces. In nowadays battlefield, forces that lose capability for high tempo will become an objects of targeting process and could be easily engaged with fire, e.g. as it happened with Ukrainian troops in the Battle of Ilovaisk 2014 [6].

Indirect fire coordination is one of the most time-critical subservices of BNS. It consists of identifying a target, identifying friendly forces near the target, selection of weapon system and firing method, engagement with fire and battle damage assessment (BDA). All well planned and conducted engagements with fire are synchronized with maneuver. Indirect fire is used to suppress enemy forces while maneuver unit closes into striking distance or conducts a maneuver to a better firing position in order to destroy targeted enemy unit. Indirect fire is used to suppress enemy's units until last moments before decisive strike, to minimize its ability to fire back or to take any countering action. That means indirect fire is used in close distance of own units.

In a battle, changes in environment and enemy actions could lead to changes of friendly unit's plans. Therefore, maneuver units have to be able to coordinate the use of indirect fire, e.g. prolong firing on enemy's position if own units movement is halted due to an obstacle, or stop fire if cap between striking position and enemy unit has closed quicker than anticipated, or move fire to previously unexpected and unplanned target. Every change in indirect fire plan has to be communicated to the firing unit without a significant delay. If a maneuvering unit sends out a correction to change fire plan but that correction is not received by the firing unit, the situation could result with a discord of a maneuver plan and a fire plan, leading to excessive losses of combat force. In MANET, both hidden terminal problem and node outage problem are supplementing to an error bool that could lead to system failure to provide indirect fire coordination between maneuver units and combat support units.

So far, the report has been describing possible hypothetical problems with MANET that affect QoS in BNS. The second part of this chapter hardware that could be used in MANET, is being discussed. In this report, we are going to compare four military MANET radios currently on the market:

1) Harris AN/PRC-158;
2) Wave Relay MPU5;
3) Streamcaster 4200;
4) R&S M3TR.

Harris AN/PRC-158 (**Figure 2**) is a modular two-channel radio that covers 30-2500 MHz frequency range. Radio works simultaneously on two channels. It is able to send and receive signals on both of its channels while working either narrowband or wideband. Embedded GPS receiver allows to present local position and to report that position. PRC-158 could use bandwidth in wideband either 1.2 MHz or 5 MHz. For practical reasons specified later in this report, we have to use smaller bandwidth in comparison with other radios [7].

Figure 2. Harris AN/PRC-158.

Wave Relay MPU5 (Figure 3) is radio specifically built for MANET. MPU5 has onboard Android OS and is highly customizable. It covers 1350 - 1390 or 2200 - 2500 MHz. Its software configurable bandwidths are 2.5, 5, 10, 20 or 40 MHz. Again, for practical reason we have to take into comparison with other radios the smallest bandwidth value [8].

Streamcaster 4200 (Figure 4) is a radio designed for low intensity conflict environment. It has currently only rudimentary functionality and would need further product development in order to suit for a battlefield. Nevertheless, Streamcaster 4200 promises to guarantee more than 100 Mbps throughput while maximum channel bandwidth is only 20 MHz. Currently smallest bandwidth in

Figure 3. Wave Relay MPU5.

Figure 4. Streamcaster 4200.

use with Streamcaster 4200 is 5 MHz, although the company producing the radio has already acknowledged that smaller bandwidth is needed and development towards that is taking place [9].

R&S M3TR (Figure 5) is a military MANET radio family that is considered to be one of the best of its kind on the market. M3TR is software defined multiband radio covering frequencies 1.5 - 512 MHz, with programmable bandwidth. Compared with other radios, M3TR data rate is lower—up to 72 kbps. In realistic, BNS that kind of low data rate could be an important restriction [10].

Table 3 shows comparison of different radios average maximum communication distances (calculated from power output or taken from information provided by producing companies) and their responding bandwidth or data rates. As Table 3 shows, all MANET radios would fit into AO of company (as showed in Table 2), 3 km being the shortest communication distance. PRC-158 and M3TR could be used in battalion AO, if that AO stays compact and does not extend in any direction. Author's personal experience has been that this is seldom true. Spread effect on a battlefield also leads to occasional widening of AO-s, forcing battalions to fight with separate companies all over a battlespace. Therefore, we could conclude that local MANETs have to be created on company level. As pointed out previously, local MANETs are connected to BNS through gateway, where for every local MANET there is one gateway. Applying that to the

Figure 5. Rhode & Schwarz M3RT radios.

Table 3. MANET radio comparison.

MANET radio comparison				
Parameters	*Radios*			
	PRC-158	**M3TR**	**MPU5**	**SC 4200**
Distance (km)	10	10	3	3 - 5
Bandwidth/data rate	1.2 MHz	72 kbps	2.5 MHz	5 MHz

amount of separate subunits operating in Brigade AO, one could calculate that there is approximately 33 - 35 gateways in BNS for local MANETs [11].

For military operations, there is generally a great need for radio spectrum availability. Units compete for same frequencies with each other and with civilian sector. Furthermore, in conventional warfare, both sides often compete for the same spectrum. Therefore, in communication plans, every channel should use as narrow part of spectrum as possible. Spectrum is also affected by restrictions of frequencies coming from LOS requirements. LOS requirements are affected by spread of units (Table 2). Use of high frequencies would refrain communication distances. For practical purposes that narrows down frequency range usable, in turn raising the competition for channel spacing. Taking into account amount of local MANETs and different networks created, one could conclude that bandwidth used in MANET should be optimized as narrow as practically possible, therefore, MANET radios should use in known spectrum environment only narrower wideband bandwidth. This is the reason behind selection of bandwidth/data rate in Table 3. Author is presuming that spectrum usage consideration is also the reason why Streamcaster 4200 is being developed to work with narrower bandwidth than current product is capable of.

Although data rate that end-user consumes for subservices, depends on a protocol, for the purpose of general comparison let's equalize it with bandwidth. Therefore,

$$1\,\text{MHz} = 1\,\text{Mbps}.$$

That kind of generalization would allow comparing data rate needed for different BNS subservices, with data rate provided by MANET radios'. Adding up data rate needed for different subservices shows that for all subservices to reach to one node seamlessly, approximately 20 Mbps of channel capacity are required (Table 1). Comparison of data rate requirement with practical bandwidth shows that there is approximately 20 times less bandwidth available in realistic architecture of BNS. Therefore, during the building phase of BNS, protocol has to be developed that:

1) prioritizes traffic on transport layer for safety-critical subservices;
2) optimizes channel use for different subservices;
3) restricts subservices on the basis of need.

Optimization means that there is probably low resource left in the system for sudden load surge if some nodes are going out of service—result of node outage problem. Therefore, node outage problem in BNS has to be addressed.

3. Analysis of System Dependability

Node outage problem is a well-known MANET problem. It is defined as a situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outage by providing an alternate route [12].

There are many ways to calculate MANET reliability, in this report terminal-pair method perfected by M. Ahmad and D. K. Mishra is used in order to describe reliability change in BNS. Terminal-pair reliability is defined as the probability of successful communication between any two selected terminals. BNS could be imagined as a sequence of a number of NLNs, where NLN is node-link-node connection. Those nodes in NLN have some independent working/operational probability [2]. In NATO countries, unit or set of fighting platforms is considered to be destroyed (defeated) if that unit has suffered more than 30% of losses. Let us assume that if military unit is destroyed, so is node corresponding to that unit. Destroyed unit would be removed from a battle for re-staging. Therefore, if we are considering only reason for node to stop working a damage during a battle, node operational working probability (Pn) is greater than $2/3$.

$$\frac{2}{3} < Pn < 1 \tag{1}$$

Link existence probability affects NLN probability, being dependent on operational status of connecting nodes. Link is operational when two nodes are in each other's transmission range. Therefore, the probability of link existence is the probability that two nodes reside in each other's range [2]. Probability for any possible link (Pl) is between 0 and 1.

$$0 < Pl < 1. \tag{2}$$

Probability of any NLN ($Pnln$) is:

$$Pnln = Pn_1 * Pn_2 * P_1. \tag{3}$$

Pn_1—operational probability of 1st node;

Pn_2—operational probability of 2nd node;

Pl—probability of link existence.

Considering average probability of node being operational, in further calculations $Pn \approx 0.83$.

Network comprises in total of E number of all possible sequences, where E is:

$$E = n(n-1)/2. \tag{4}$$

Reliability of a particular configuration (Pc) is the product of all possible individual NLN probabilities:

$$Pc(t) = \Pi_1^E (Pnln)^{Lt} (1 - Pnln)^{Lt} \tag{5}$$

$Lt = 1$, if the link exists in the current NLN, and

$Lt = 0$, if link does not exist.

$$\Sigma_i^E = 1 Pc = 1. \tag{6}$$

Previous equation represents the sum of all configuration probabilities, where $e = 2^E$. To calculate the two-terminal reliability of the network for any two nodes, we are using:

$$2TR = \Sigma_i^E = 1Pc * Pi \quad (7)$$

$Pi = 1$, if at least a single path exists between selected two nodes;

$Pi = 0$, if it does not exist.

Not all links exist with same probability. The nodes which are closer to each other have higher probability of link formation than nodes which are n-hops apart. MANET usually have a peer-to-peer communication scenarios, rarely creating unique multiple redundant paths between two nodes, therefore, existence of a critical node is almost certain in any MANET. A configuration with critical node has higher load leading to higher probability of link failure [2]. To detect critical nodes in any given configuration we have to use DMCC algorithm introduced by M. Sheng, J. Li and Y. Shi [13]. Simplified description of DMCC would allow selecting a pair of nodes in local MANET, which are two-hop nodes. Then all possible global paths of those nodes have to be found. If all paths of selected nodes include one certain third node, then that verifies that third node as a global critical node.

After detecting global critical nodes, M. Ahmad and D. K. Mishra algorithm could be used to calculate total two-terminal reliability from source node up the first node of the current NLN. Then all individual sub-network reliabilities and the individual reliabilities of all critical NLN-s have to be multiplied to calculate the final reliability of this network configuration [2].

In this report, it is not feasible to calculate overall reliability for BNS due to the fact that Brigade is a very large unit with lot of subunits (model of Infantry Brigade consists of 278 important agents, excluding most of combat service support subunits [11]). Prior to the calculation of configuration of reliability, configuration model has to be created. For that purpose every subunit and every node has to be described. This is not possible due to the fact that BNS itself does not exist yet. Therefore, in this report set of local MANETs is described for reliability calculations, in order to illustrate QoS change in BNS during an operation.

With a network comprising of ~500 nodes, E (total number of all possible NLN sequences) would be equal to 124,750. But as stated before all those nodes will not be in communication distance of each other. For reliable calculations smaller network, local MANET has to be described. Let us assume that there are two maneuver companies operating side by side. Both are with equal set of nodes. Companies belong to different battalions; therefore, they use normally a different route to the BNS. Let us also assume that both of those companies have critical link to overall BNS through gateway operating on company level (**Figure 6**).

In this system two critical links exist. As stated before, link exist's if two nodes are in each other transmission range. For comparison, let's first state that $Pl < 0.5$, thus average $Pl = 0.25$. Let us assume that all nodes in local MANET are in each other communication range. Total number of nodes in this example is 26.

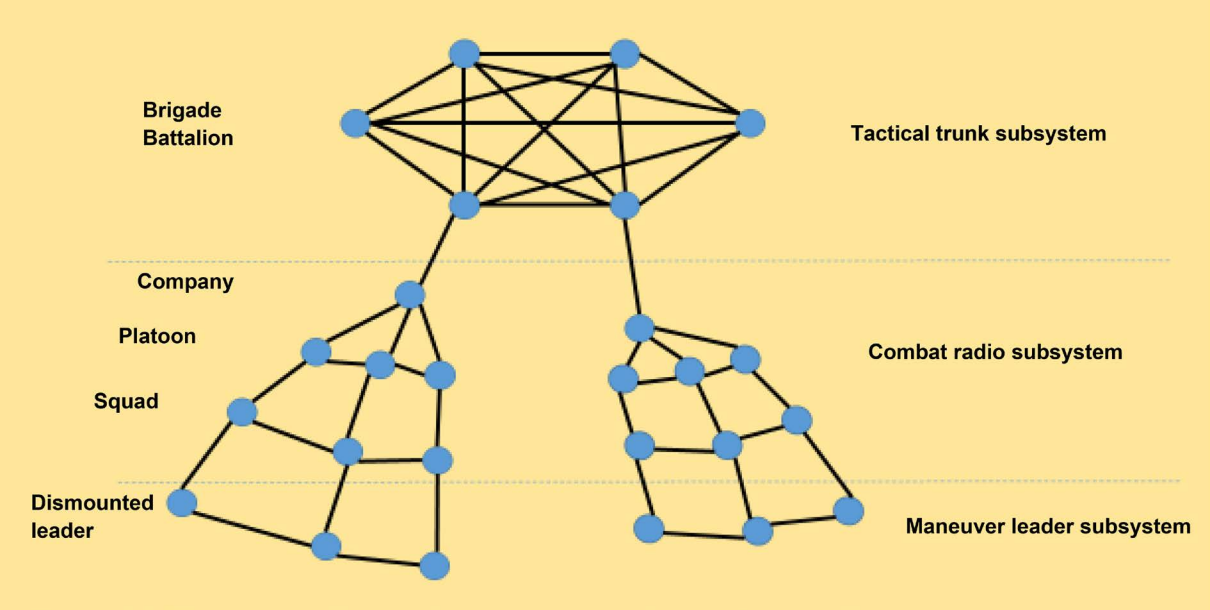

Figure 6. Company-level local MANETs in BNS.

Therefore,

$$E = 325.$$

For every given NLN, with $Pl = 0.25$, $Pnln = 0.17$.

If all links between any given two nodes exist with same probability, then we could simplify reliability calculation of a particular configuration as follows:

$$Pc(t) = \left((Pnln)(1-Pnln)\right)^{a} \tag{8}$$

where a = number of NLN steps going through critical link. It represents a route from one cluster to another in order to ensure equal information in nodes in both clusters. In our example $a = 5$. Therefore,

$$Pc(t) = 5889 \times 10^{-5}. \tag{9}$$

Now let's change Pl value: $Pl = 0.5$. Thus:

$$Pc(t) = 0.000587. \tag{10}$$

If we set Pl value to 0.75, then:

$$Pc(t) = 0.000971. \tag{11}$$

Figure 7 shows $Pc(t)$ value change in BNS, where x-axis represents change on Pl value and y-axis change in $Pc(t)$ value. As stated before, configuration with critical node leads to higher load, which in return leads to higher failure rate. That means that more hops there are in a particular system, less reliable it is.

Hypothesis can be verified by changing "a" value. If $a = 2$, then:

$$Pc(t)^{n} = 0.062361 \tag{12}$$

$Pc(t) < Pc(t)^{n}$, therefore, it has to be concluded that amount of hops signals

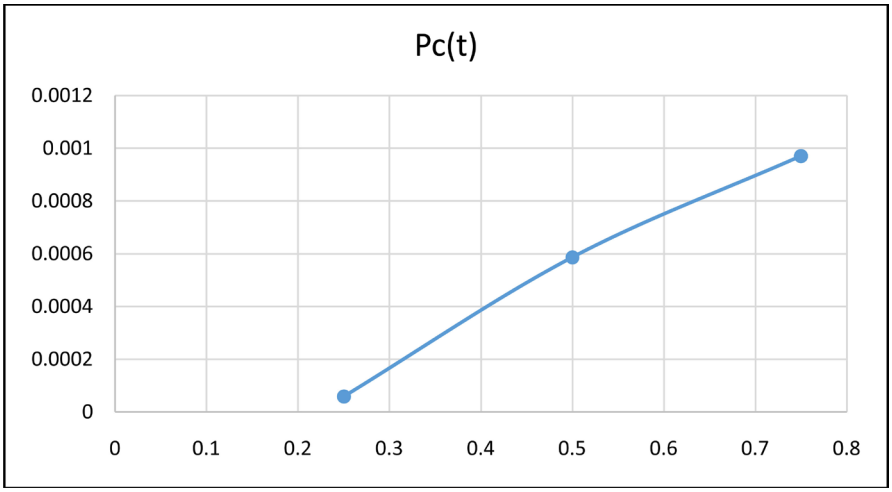

Figure 7. $Pc(t)$ change in BNS.

require in a system affects reliability of a system.

In our example of two companies, both company's local MANET has $E = 45$ different ways to configure the network. Let's assume that edge-node has to take minimum two hops to reach a gateway (due to the change in environment). If in this network amount of NLN connections shrinks, then at some point a new critical link will be formed. Pl value will lessen, therefore, lessening configuration reliability.

D. Zhang and J. P. G Sterbenz research [14] shows that with the increasing number of simultaneous node failures, the performance difference between critically linked part of a system and well linked part of a system becomes smaller. Therefore, one could conclude that as many nodes of BNS as possible should be able to form a new gateway to tactical trunks subsystem or to neighboring clusters.

Concept of BNS implies that node outage happens not only due to the damage, but also when tactical trunk subsystem node changes its position. In this case traffic from corresponding companies has to be diverted to neighboring gateways. That in turn will increase error rate of transport layer, because errors mostly occur when alternative routes exist but are relatively long, and therefore, may not provide satisfactory service in application [15].

As one could see, node outage problem has a major effect on QoS in BNS. Coming back to safety-critical dependability issues on a battlefield, one has to ask how this affects our understanding of a reliability of a system. As an example with local MANETs and two companies showed, with many critical links in a system overall reliability of a systems ability to provide safety-critical subservices for every node in a system is relatively low. One could say that due to the fault in system design, error that could lead to catastrophic failure is bound to happen. Therefore, it is this report's authors opinion that even in future battlefield Fire Support Coordination Measures have to be in place, separating and de-conflic-

ting maneuver and fire of different subunits. Another option would be to calculate every node's possible position, taking into account where its last coordinates were, what is its practical possible speed, etc. But this could mean that a new subservice has to be created in BNS service layer, increasing the burden on transport layer even more.

Increase of critical links increases work load and could disrupt BNS ability to manage traffic in transport layer. One has to keep in mind that due to service layer and transport layer data rate differentiation protocol developed for BNS is probably already using transport layer resources as efficiently as possible. Thus protocol should be able to react to significant change in transport layer. Due to limited resources of transport layer, service differentiation has to be created and safety-critical subservices priority has to be granted.

4. Conclusions

In this report, the concept of future Battle Network System was introduced. Due to the fact that most of BNS transport layer could be described as MANET, the report evaluated BNS transport layer's ability to maintain Quality of Service through known MANET problems, using MANET evaluation analysis techniques. Although report findings could be counted as intuitive truths, in author's opinion, they still have a value for system developers, namely helping to state the problems and steps to solve those problems.

MANET is probably the best choice for BNS transport layer. Nevertheless, MANET problems are going to affect BNS and have to be addressed during the development phase. First, every MANET is bound by critical links. Therefore, as many nodes as possible should be able to form a gateway to tactical trunk subsystem.

Second, nodes should be with as long communication distance as reasonably possible. That will decrease the amount of hops in BNS, therefore, decreasing error rate. Radios with longer communication distances are also able to form NLN sequences with neighboring local MANETs, thus decrease the number of critical links in the system.

Third, safety critical subservices in BNS have to have a priority and have to be superimposed by battle planning rules and Fire Support Coordination Measures. The hope, that BNS service layer of Network Centric Command (e.g. BMS) would allow to de-conflict fires and maneuvers with high accuracy and increase the efficiency of battlespace use, is not feasible without significant risk-taking.

Fourth, subservices in BNS should be restricted in the basis of need. That would lessen the burden of transport layer and would simplify the development of communication protocol.

Further research is needed to determine, what would be:

1) The suitable protocol for BNS;
2) Reasonable bandwidth in realistic spectrum environment;

3) Possible alternatives to ensure that errors in safety-critical subservices would not lead to a failure.

For the next step, parts of BNS transport layer and service layer have to be created. Transport layer could be a rudimentary set of nodes, which it does not need to represent the whole BNS. But in author's opinion, the service layer should be as complete as possible in order to be able to provide realistic traffic for transport layer. Then a realistic scenario for simulation has to be created. Scenario should not only provide traffic, but also address different errors. Different sets of node outage problems have to be tested during simulation. Measurements will show possible faults in BNS architecture, allowing making corrections during system design phase.

References

[1] Innos, R. (2009) Võrgupõhise sõjapidamise teooria ja selle rakendamise võimalused Eesti Kaitseväes. MPhil Thesis, ENDC, Tartu, 65.

[2] Majid, A. and Mishra, D.K. (2012) A Reliability Calculations Model for Large-Scale MANETs. *International Journal of Computer Applications*, **59**, 17-21.

[3] Mõts, E. (2010) Eesti Kaitseväe maaväe lahingutegevuse alused. ENDC, Tartu, 85-88.

[4] JP 3-09, Joint Fire Support. (2014). p (I-4).

[5] Zhai, H. and Fang, Y. (2006) A Solution to Hidden Terminal Problem over a Single Channel in Wireless Ad Hoc Networks. *IEEE Military Communications Conference* (*MILCOM* 2006), Washington DC, 23-25 October 2006. https://doi.org/10.1109/MILCOM.2006.302394

[6] Sinclair, N. (2016) Old Generational Warfare. The Evolution—Not Revolution—of the Russian Way of Warfare. *Military Review*, May-June 2016, 15.

[7] Harris Falcon III AN/PRC-158, Multi-Channel Manpack Radio Data Sheet. (19.05.2016) http://rf.harris.com/media/Harris%20AN-PRC-158%20Data%20Sheet_tcm26-25154.pdf

[8] Wae Relay MPU5. (19.05.2016) http://www.persistentsystems.com/site/wp-content/themes/persistensystems/pdf/mpu5/mpu5_spec_sheet.pdf

[9] Streamcaster 4200 MANET Radio Data Sheet. (19.05.2016) https://drive.google.com/file/d/0B6nR1O6OfjRrcmNNbXpYODVpTnM/view

[10] Rhode & Schwarz Software Defined Radios M3RT. (19.05.2016) https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/M3TR-family_bro_en_5213-9228-12_v0500.pdf

[11] Dieves, V. (2016) Jalaväebrigaadi olukorrateadlikkuse staatiline mudel. Unpublished Study, ENDC, Tartu.

[12] Pathan, A.S.K., Lee, H.-W. and Hong, C.S. (2006) Security in Wireless Sensor Networks: Issues and Challenges. *Advanced Communication Technology* (*ICACT* 2016), Phoenix Park, Korea, 20-22 February 2006, 6.

[13] Sheng, M., Li, J. and Shi, Y. (2006) Critical Nodes Detection in Mobile Ad Hoc Network. IEEE Computer Society, Conference Paper.

[14] Zhang, D. and Sterbenz, J.P.G. (2014) Modelling Critical Node Attacks in MANETs. In: Elmenreich, W., Dressler, F. and Loreto, V., Eds., *Self-Organizing Systems*, Springer Berlin Heidelberg, 127-138. https://doi.org/10.1007/978-3-642-54140-7_11

[15] Jorgic, M., Stojmenovic, I., Hauspie, M. and Simplot-Ryl, D. (2004) Localized Algorithms for Detection of Critical Nodes and Links for Connectivity in Ad Hoc Networks. *Proceedings of the* 3*rd Annual IFIP Mediterranean Ad Hoc Networking Workshop*, Turkey, 12.