Application of Dezert-Smarandache Theory for Tactical MANET Security Enhancement

Joanna Głowacka, Marek Amanowicz
Faculty of Electronics
Military University of Technology
Warsaw, Poland
{jglowacka, mamanowicz}@wat.edu.pl

Abstract—**The article presents a concept of Dezert-Smarandache theory application for enhancing security in tactical mobile ad-hoc network. Tactical MANET, due to its specification, requires collection and processing of information from different sources of diverse security and trust metrics. The authors specify the needs for building a node's situational awareness and identify data sources used for calculations of trust metrics. They provide some examples of related works and present their own conception of Dezert-Smarandache theory applicability for trust evaluation in mobile hostile environment.**

Keywords- situational awareness, trust, inference methods, tactical MANET, security, Dezert-Smarandache theory

I. INTRODUCTION

The mobile ad-hoc networks are collections of independent nodes that can communicate via radio channels. These networks are often developed in conditions of limited or total lack of access to fixed infrastructure.

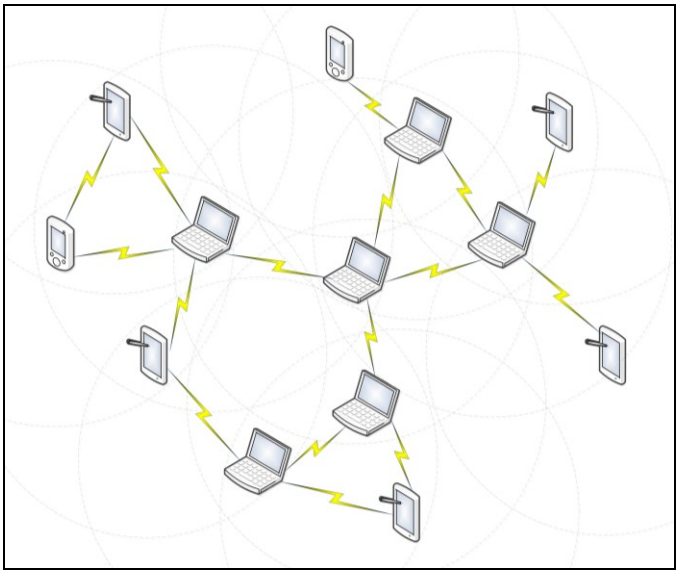

Figure 1. A sample mobile ad-hoc network structure

MANETs are characterized by high dynamic changes in the location of each node and the vulnerabilities of various types of attacks. Due to the open medium, ad-hoc networks are more susceptible to eavesdropping and data injections. A dynamic change of network topology contributes to the frequent connecting and disconnecting nodes, and no central network monitoring makes it difficult to detect malicious behaviour of nodes. In addition, the network resource limitations contribute to the selfish attacks. They are aimed at consuming a large amount of bandwidth. One of the selfish behaviours is the failure to transfer the packages by a node to conserve its own energy.

Security ensuring is particularly difficult for a tactical ad-hoc network, due to the necessity of dealing with a hostile environment, strict capacity constraints, the requirements for services, very rapid changes of network topology and dynamically forming groups of common interests, which cannot be pre-defined by trust relationships [1]. These networks are characterized by simple capability of adding new nodes, which may be of diverse nature, such as the allies, neutral or hostile nodes.

One method of ensuring the security is user authentication. Only the authorized nodes and those verified as allies can have access to the network. However, during the mission, a node can be taken over by the enemy, or change the nature of its behaviour - behaving to the detriment of the mission.

Due to the lack of a central management system it is needed for nodes to cooperate. Each of them is in fact a router ensuring cooperation between subnets and nodes located at a distance greater than the radio range.

Restrictions on ad-hoc networks contribute to the need of using other means than in wired networks to satisfy the safety requirements. In addition to authorization and authentication mechanisms, it is necessary for a node to have the knowledge on the behaviour of other nodes in the network, determining safety routes for data transfer and knowledge concerning the reaction manners in certain situations. The situational awareness building method will be complement of standard security mechanisms in mobile ad-hoc networks.

II. NODE'S SITUATIONAL AWARENESS

A. Definitions

To identify opportunities of secure cooperation between nodes in ad-hoc networks, it is necessary to collect information about other nodes in the network. The ability to have accurate information about the surrounding reality and interpretation of the current situation in terms of the performed tasks is defined as a node's situational awareness.

This article was written as a part of a scientific research project financed by polish government budget for science in 2010 ÷ 2013 "An advanced methods and techniques of traffic control in tactical ad-hoc networks" No. O N517 274 839.

The main product of the node's situational awareness mechanism is information on the node trust levels.

Trust is an interdisciplinary concept, characterized by a variety of definitions. It is understood as relying on the integrity, strength and ability of a person or thing. In the case of ad-hoc network it is translated as a set of relationships between people who use similar communication protocols [1]. These relations are defined based on previous interactions of individuals. In [2], trust is treated as the degree of belief about the behaviour of other entities. Trust can also be understood as reputation, opinion, or the probability of correct behaviour [3].

In MANET, trust is the level of faith, which can be assigned by the node to its surroundings on the basis of observations and opinions coming from the other nodes in the network [4].

B. Benefits

Building node's awareness is essential to achieve the mission. In heterogeneous networks, the completion of the mission is dependent on the integrity of individuals. The knowledge gained from building node's awareness can ensure cooperation only between trusted entities that do not behave suspiciously.

Secure exchange of information between nodes requires proper selection of the route of data transfer. Sending data via routes that are not safe may contribute to the leak or acquisition of data by unauthorized persons. Lack of metrics allowing for choosing the path depending on the level of confidence in nodes and the risk, that exists in choosing the path of data transfer and cooperation between the nodes, may contribute to the failure of the operation.

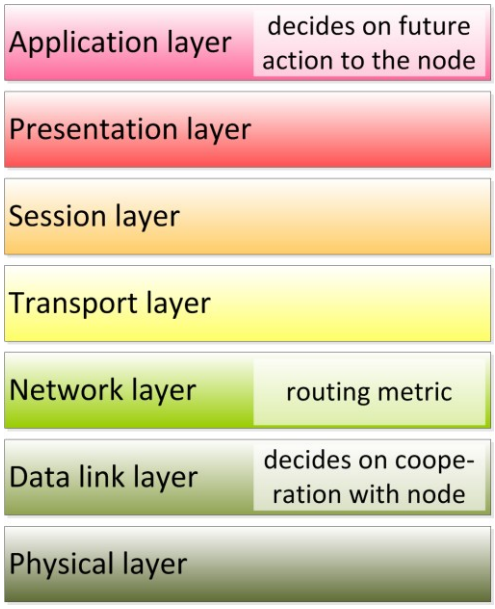

Figure 2. The possibility of application of the knowledge from building node's awareness in different OSI model layers

The dynamic process of creating a current situational view of node can be the basis for decisions on how to control traffic.

The knowledge about the surrounding environment gained through the mechanism of building node's awareness can be applied in different layers in order to protect the communication between nodes. In the data link layer it can be used to define a parameter indicating the possibility of cooperation with the nodes or the need for failure to communicate with nodes characterizing a low level of confidence. In the third layer level of trust, it can be used as metric routing protocol that will allow you to safely share data. Specified nodes confidence level can be used also in the application layer, where the nodes of questionable confidence level will be forced to certain behaviour for performing its final assessment assignment.

C. Data sources

Node's situational awareness in most cases is built based on direct interactions, indirect observations and recommendations.

Trust determined by the node based on direct interaction and observation of behaviour of other nodes is called direct trust.

Trust determined on the basis of indirect observations and recommendations is called indirect trust. Recommendations shall be understood as opinions of other nodes on the node for which the level of confidence is being specified.

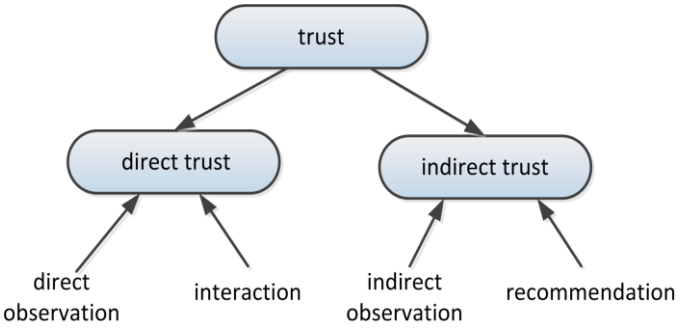

Figure 3. Direct and indirect trust

In many cases information from various sources may be incomplete, inconsistent or conflicting. This requires the selection of appropriate methods of inference, which would allow clear and accurate assessment of the current environment in which network node operates.

III. RELATED WORKS

The problem of gathering information about the surrounding node reality and determining the nodes trust in ad-hoc networks has recently been very popular and widely developed in the literature, which demonstrates the importance of this topic.

Probabilistic inference is the most frequently used method in the literature to determine the node trust level. The information about node behaviour is evaluated as 0 or 1, match or success.

In [5], the theoretical concept was presented to assess the level of trust and its propagation. Trust in this approach is considered as a measure of uncertainty expressed in a measure

of entropy. In the case of entropy based trust model, promoted trust is calculated on the basis of individual trust values. In the trust model based on the probability, the value of propagated trust is calculated by the probability of trust relationships. In this model, the probability of correct relations assessment is also included. This concept also includes an assessment of trust on the basis of observation.

In [6], new concept of the TMF (Trust Management Framework) was presented. TMF is used for nodes to obey protocol and cooperate with each other. There are two types of TMF:

- reputation based - trust is assessed based on direct observations and information of the second hand, Bayesian approach based on the distribution of β is being used,
- trust establishment - trust is assessed based on direct observation and the relationship established between nodes without regard to previous opinions of intermediate nodes.

Both types of TMF are immune to numerous attacks, therefore, OTMF (Objective TMF) has been proposed to prevent them. This solution is based on modified Bayesian approach, in which different weights are assigned to different information given at the time of their occurrence and that concerning their supplier. Influence of the previous observations decreases exponentially, and the trust is used as a weight for second-hand information. The two parameters - "trust value" and "confidence value" - are combined in OTMF into one metric called "trustworthiness".

The article [7] presents Hermes framework determination of node trust, which helps in ensuring the reliability of packet transmission. Framework ensures that the source sends packets only by the trusted intermediate nodes. In this solution, each node determines the reliability metric of neighbouring nodes based on direct observation of transmitted packets. Reliability is further extended with opinions from other nodes. The proposed solution uses a Bayesian approach to determine the value of trust. Trust is calculated on the basis of the beta probability distribution. Beta distribution parameters are determined from observations gathered during the packet forwarding behaviour. A new metric called trustworthiness, being a combination of trust and confidence metrics, is introduced.

In [8], the trust model was created for the DSR protocol in order to take a decision on acceptance or rejection of the route. Decisions are made based on the estimated trust respectively. Trust is determined on the basis of the direct trust and recommendations from other nodes. Direct trust is determined by the sum of experiences on a given node and the recommendation trust is the sum of the recommendations received from the nodes. In determining the total trust value both values are taken into account, but the direct trust has the higher weight. Direct trust is determined by observation of packets forwarded by the evaluated node. Collected observations are evaluated positively if they are not modified. The assessment is proportional to the type of transmitted packet (e.g. route request, data packet). If sent packages are modified, the observation is evaluated negatively. Negative evaluation is proportional to the type of packet transmitted and the type of modification (e.g. modification of information about the source, recipient, sequence number, route).

The use of probabilistic inference provides an easy way to determine the node trust level but also has some disadvantages. Classical logic is based only on two values represented by 0 and 1 or true and false. The border between them is clearly defined and unchanging. In addition, classical probability theory does not allow for distinguishing uncertainty (expressed in terms of probability) from incomplete knowledge (lack of knowledge on the topic).

The other inference method used to evaluate and combine knowledge about node behaviours is fuzzy logic.

Trust model based on the recommendation similarities (RFSTrust) calculated with the use of fuzzy mathematics for MANET environment was presented in [9]. The fuzzy trust model is proposed to quantify and evaluate the trustworthiness of nodes, which includes five types of fuzzy trust recommendation relationships. Theoretical analysis and the simulation results show that RFSTrust model can effectively prevent selfish nodes and improves the performance of the entire MANET.

As in the case of inference based on classical logic, fuzzy inference does not allow separation of uncertain knowledge from lack of knowledge.

Another method of enabling the representation of uncertainty is the mathematical theory of evidence.

The use one of the mathematical evidence methods – the Dempster-Shafer theory (DST)[10] - for the determination of selfish behaviour of each node is presented in [11]. Node cooperation rating is based on the observation of correct packet delivery. If a source node receives the information about arrival of the package, it will mean that all nodes in the path behave correctly. In this case, the source node defines the m() function for each path node, which is named basic belief assignment, as:

$$m(A) = \begin{cases} 0 & A = \{SELFISH\} \\ 1 & A = \{UNSELFISH\} \end{cases}. \quad (1)$$

In the absence of proof of information delivery and the lack of error messages, the source node finds that a path includes not cooperating nodes. Unfortunately, a number of these nodes and information about which nodes are selfish is not known. The basic belief assignment is defined as:

$$m(A) = \begin{cases} P & A = \{SELFISH\} \\ 1-P & A = \{UNSELFISH, SELFISH\} \end{cases}. \quad (2)$$

Each of the nodes in the network is equipped with a dedicated component implementing an algorithm based on the Dempster-Shafer theory, which uses the received recommendations and results of nodes observation. The solution has defined two types of trust. The first determines the extent to which the source node trusts another node that it will send the package correctly. It was used to determine the belief function defined by the Dempster-Shafer theory. The second value indicates the degree of trust in which a node trusts that recommendations generated by another node are correct.

IV. CONCEPT DESCRIPTION

Dynamic evaluation of the environment surrounding the node is possible by continuously monitoring the node behaviour, their analysis and information inference.

Figure 4. Node evaluation process

In many cases, the knowledge acquired by a single node is insufficient to fully assess the current situation, therefore it must be able to exchange information about situational awareness built between nodes. Nodes can have different access to data about other nodes, so their passing information may be incomplete or uncertain. In the solutions described in section III, in most cases it is impossible to distinguish ignorance from uncertain knowledge, taking into account incomplete and conflicted knowledge derived from various sources.

The Dezert-Smarandache theory [12-14] allows combining information from multiple sources. It focuses on the problems of combining uncertain, conflicted and inaccurate information [15]. DSmT overcomes the limitations of applying the inference methods used so far in the assessment of trust: probabilistic inference, fuzzy logic or DST. These methods enable the binary evaluation of nodes or creating hypotheses that cannot penetrate. By using DSmT it is possible to create any number of hypotheses that do not have to be exclusive, and thus more accurate assessment of the nodes. In addition, this method enables to distinguish the uncertain knowledge from ignorance.

This theory rejects the main limitations of the Dempster-Shafer theory:

- frame of discernment is a finite, exhausted and exclusive set of hypotheses,
- the application of the excluded middle rule,
- acceptance of the Dempster's rule as a rule a combination of views,
- acceptance of the Dempster's conditioning rule.

The DSmT distinguished two types of models:

- free model - where frame of discernment (Θ) consists of extensive but not exclusive items, so components can be mutually overlapping. This model is called free because of the lack of assumptions imposed on the hypothesis.
- hybrid model – it allows the modelling of imprecise-views and exclusivity constraints Θ elements. In this case, the elements may overlap, but they do not have to.

The DSmT introduces the concept of hyper-power set, which is denoted by D^{Θ}. This collection is understood as the set of all proposals that were created from elements of Θ with the use of operators $\cup$ and $\cap$. For example:

$$\text{for } \Theta = \{\theta_1, \theta_2\} \Rightarrow D^{\Theta} = \{\alpha_0, \alpha_1, ..., \alpha_4\}, |D^{\Theta}| = 5$$
$$\alpha_0 = \varphi, \alpha_1 = \theta_1, \alpha_2 = \theta_1, \alpha_3 = \theta_1 \cap \theta_2, \alpha_4 = \theta_1 \cup \theta_2. \quad (3)$$

A. Events monitoring

Node assessment is made based on direct node observation and information from neighbouring nodes. Examples of observed events by which nodes can be evaluated are:

- provision of information - some of the nodes in ad-hoc networks are characterized by self-interested behaviour in order to deprive other nodes of the shares, for example by failing to forward packets for selfish node to the other nodes. Validation of packet transmission is possible through the analysis of incoming acknowledgments, when transmission of acknowledgments is enabled in the network or by tracking the packages sent by the monitoring node.
- compliance of safety rules - in tactical networks information may have different levels of sensitivity, for example: secret, confidential, non-confidential. Data on a certain level of sensitivity can be sent only to nodes that have access to information about a specific level or a higher level. Based on information collected on nodes access levels and data contained in the labels, it can be verified if a node observes the principles of safety, i.e. whether it has access only to data which is authorized and makes it available only to the authorized users.
- recommendation correctness - in the case when trust level is determined by recommendations from other nodes in the network, it is necessary to provide protection against “liar” nodes. A “liar” shall construe nodes, which transmit incorrect recommendations on other nodes, the objective of re-routing packet forwarding, intercepting or preventing delivery to the destination node.

The observed events can be evaluated as 0, 1 - using the classical theory of probability. However, in many cases, the observed behaviour provides some indication of both hypotheses, which would require omitting the evaluation of the event or a need to assign two assessments - which would misrepresent the two behaviours. Each behaviour is treated equally and the designated level of trust makes it impossible to identify the appropriate response to behaviour.

B. Nodes classification

Application of the Dezert-Smarandache theory provides for more hypotheses, which enable more accurate assessment of behaviour. Additionally, through the creation of secondary hypotheses using sum and product operators, it can constitute representation of imprecise and uncertain hypotheses.

During the observation of nodes behaviour they can be evaluated as:

- cooperating node (C) - the node transmitting information,
- egoistic node (E) - the node is not transmitting information,
- honest node (H) - the node transmitting the proper recommendations,
- liar node (L) - the node transmitting incorrect recommendations,
- secure node (S) - the node adhering to safety rules,
- unsecure node (U) - the node is not adhering to safety rules.

The set of basic assumptions in some cases may be insufficient for correct classification of nodes. Apart from the hypotheses, it is possible to determine the basal intermediate hypotheses developed from the basal hypothesis with the sum and logical product operators. The secondary hypotheses can distinguish:

- uncertain cooperating node (UC) - the node to which correctness of packet forwarding was tested, but it is not possible to take clear decision whether it is a cooperating or selfish node. This situation can occur if a node did not receive confirmation of the package transfer - for each of the nodes in the path the uncertain cooperating node hypothesis is taken.

$$UC = C \cup E$$

- suspect liar node (SL) - the node whose recommendations may be biased, the value reported earlier, recommendation differs from the accumulated knowledge and the other recommendations, however, this difference does not yet allow for finding that they are wrong and biased.

$$SL = H \cap L$$

- uncertain honest node (UH) - the node to which you cannot determine whether the recommendations forwarded by it are correct, because of the lack of previously accumulated knowledge.

$$UH = H \cup L$$

- suspect unsecure node (SU) - the node whose behaviour indicates partial compliance with security rules, for example, a node has access to the resources which are not eligible, but only make them available to the authorized individuals.

$$SU = S \cap U$$

- uncertain secure node (US) - the node in the case of which you cannot determine if it complies with the security rules, due to lack of knowledge regarding the node's resource access level.

$$US = S \cup U$$

With such specific hypotheses, it is possible to refine the assessment of nodes indicating the possibility of exchanging data with the node, but it does not include an incoming recommendation and needs more detailed observation of node's behaviour, for example by using an additional mechanism for including a node to certain behaviours.

C. *Sample evaluations*

Information fusion is done separately for each type of event - co-operation between the nodes- following the security rules and recommendation correctness. Each hypothesis is assigned with a value of m(), depending on the number of observed events, which were assigned to a particular hypothesis. The m() is described by conditions defined by the following formula (4):

$$\begin{aligned} m(\phi) &= 0 \\ \sum_{A \in D^{\Theta}} m(A) &= 1. \end{aligned} \tag{4}$$

The set of hypotheses for each type of event allows using the DSm rule of combination for free-DSm models:

$$m_{M(\Theta)}(A) = \sum_{\substack{X_1, X_2, \ldots X_k \in D^{\Theta} \\ (X_1 \cap X_2 \cap \ldots \cap X_k) = A}} \prod_{i=1}^{k} m_i(X_i). \tag{5}$$

Tables 1 and 2 show some example values of the received recommendations on node's cooperation observation and compliance with security policies.

TABLE I. RECOMMENDATION ABOUT NODE COOPERATION

	cooperating	egoistic	uncertain cooperating	suspect egoistic
m_1	0,650	0,030	0,320	-
m_2	0,720	0,050	0,230	-
m_3	0,690	0,040	0,270	-
$\boldsymbol{m_{M(\Theta)}}$	**0,865**	**0,011**	**0,020**	**0,105**

TABLE II. RECOMMENDATION ABOUT SECURITY POLICY COMPLIANCE

	secure	unsecure	uncertain secure	suspect unsecure
m_1	0,230	0,265	0,150	0,350
m_2	0,270	0,290	0,070	0,370
m_3	0,320	0,280	0,100	0,300
$\boldsymbol{m_{M(\Theta)}}$	**0,136**	**0,130**	**0,007**	**0,727**

It can be specified based on the collected recommendations, if the node is cooperating and suspect unsecure. This information allows a node to take a decision on further node observation. The node can forward low sensitivity information, whose transmission to unauthorized units will not contribute to the realization of carried out actions.

V. CONCLUSION

Ensuring security in tactical MANET requires gathering and processing information about the node surrounding reality. Information from various sources, however, is often uncertain, incomplete and even conflicting. The method ensuring coverage of all of this information is Dezert-Smarandache theory, which allows representing of imprecise hypotheses. By applying the Dezert-Smarandache theory it is possible to identify specific and general hypotheses, which can combine data from different sources with access to information on the behaviour of nodes. As part of further work a function that enables combining data including their update time and weight of data sources will be determined.

REFERENCES

[1] K. Seshadri Ramana, A.A. Chari, N. Kasiviswanth: "A Survey on Trust Management for Mobile Ad Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol. 2, No. 2, April2010.

[2] L. Capra: "Towards a Human Trust Model for Mobile Ad-hoc Networks", Dept. of Computer Science, University College London.

[3] Z. Han, K. J. R. Liu, Y. L. Sun, W. Yu: "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defence Against Attacks", INFOCOM 2006. 25th IEEE International Conference on Computer Communications, April 2006.

[4] J. Głowacka: "Procedures of building nodes' awareness for security in tactical ad-hoc networks, KKRRiT 2011, Poznań 2011, Telecommunication Review – Telecommunication News 2011 [CD], No. 6, pp. 405-408 (in Polish).

[5] Zhu Han, Yan Lindsay, K. J. Ray Liu, Wei Yu: "Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

[6] Jien Kato, Jie Li, Ruidong Li: "Future Trust Management Framework for Mobile Ad Hoc Networks", IEEE Communications Magazine, April 2008, pp. 108-114.

[7] C. Zouridaki, B. L. Mark, M. Hejmo, R. K. Thomas: "A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs", In SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 1–10, New York, NY, USA, 2005.

[8] V. Balakrishnan, V. Varadharajan, U. K. Tupakula, P. Lucs: "Trust and Recommendations in Mobile Ad hoc Networks", Third International Conference on Networking and Services, IEEE 2007.

[9] Junhai Luo, Xue Liu, Mingyu Fan,: "A trust model based on fuzzy recommendation for mobile ad-hoc networks", Computer Networks 53 (2009), pp. 2396–2407.

[10] Shafer G.: "A mathematical theory of evidence", Princeton U.P., Princeton, NJ, 1976.

[11] J. Konorski, R. Orlikowski: "DST-Based Detection of Noncooperative Forwarding Behavior of MANET and WSN Nodes", Proc. 2nd Joint IFIP WMNC., Gdansk, Poland, 2009.

[12] F. Smarandache, J. Dezert: "Advances and Applications of DSmT for Information Fusion", Vol 1, American Research Press Rehoboth, 2004.

[13] F. Smarandache, J. Dezert: "Advances and Applications of DSmT for Information Fusion", Vol. 2, American Research Press Rehoboth, 2006.

[14] F. Smarandache, J. Dezert: "Advances and Applications of DSmT for Information Fusion", Vol. 3, American Research Press Rehoboth, 2009.

[15] J. Głowacka, M. Amanowicz: „Situational awareness of a military MANET node – the basis" („Podstawy tworzenia świadomości sytuacyjnej węzła wojskowej sieci MANET"), Telecommunication Review – Telecommunication News 2012, No. 2-3, pp. 59-62 (in Polish).