Using Application of Dezert-Smarandache Theory on a new framework for protecting MANET

Ekata Gupta
Research Scholar, Mewar University

Dr.S.K.Saxena
CSE Department
Delhi Technological University(Formerly Delhi College of Engineering)

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 history of mobile ad hoc networks came back to Packet Radio Networking project in 1972 that was done by DARPA 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.

Mobile Ad hoc Network is an autonomous system of mobile devices that do not relay on any fixed infrastructure (see Fig.1). On one hand, lack of any fixed infrastructure makes these networks suitable for some critical applications such as emergency operations, disaster relief efforts, business indoor applications, civilian outdoor applications, military networks and so on . On the other hand, providing security for MANETs would be one of the most significant challenging issues.

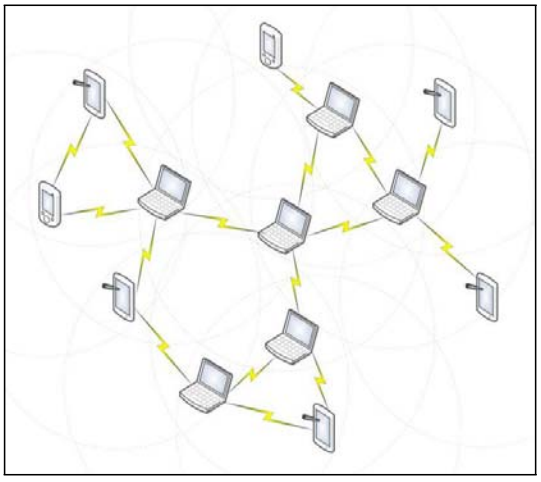

Figure 1. A sample mobile ad-hoc network structure

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. MOBILE AD HOC NETWORK CHARACTERISTICS

(a) Self-configured: Based on this feature, network functions (e.g. routing) must be done by the nodes, to keep the network usable.
(b) Dynamic topologies: Random movements of the nodes make the topology of the network unpredictable and highly dynamic.
(c) Resource constrained devices: Nodes are resource constrained in bandwidth, battery, memory, processing capability and computing power.
(d) Poor physical security: There is a possibility that mobile devices being captured or broken by adversaries.

III SECURITY ISSUES IN MOBILE AD HOC NETWORKS

Mentioned features above can lead to a set of underlying assumptions and performances and security concerns, which makes the design procedure more challenging. Due to the ability of communication over wireless channels and rapid growth of mobile devices, lack of widely accepted security solutions for this environment, made the research over security of MANETs still an active area .

Effective and proven security solutions for traditional networks are not always applicable to MANETs. In fact, attacks (e.g. identity/address spoofing, message tampering/ forgery/ replay) which may be easily detected and prevented in the traditional networks could be very challenging in MANETs. Mentioned issues in mobile ad hoc networks led to the difficulty of achieving security requirements .

Similarly to the traditional networks, MANETs need some security requirements which are described below :

(i) Data Confidentiality: keeping data secret from unauthorized entities
(ii) Data Integrity: preventing modification of data by unauthorized entities
(iii) Data Freshness: Keeping data in the correct order and up-to-date
(iv) Data Availability: Ensuring that data will be available on request
(v) Data& Identity Authentication: Verifying that the data or request is coming from a valid sender
(vi) Non-repudiation: Ensuring that a node cannot deny sending a message.

IV. 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.

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. Security risk

Security risk and vulnerabilities assessment has many benefits and challenges associated with it. The security risk assessment should provide complete view of the existing security risk and help provide alternative solution and changes to the security measures and controls. We propose that an enhancement is needed, which will improve the security risk assessment
process, and that enhancement can be made to security risk management approach

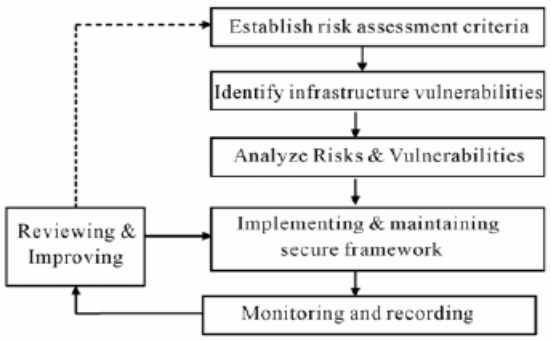

Figure 2: Security Risk Management framework

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.

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

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.

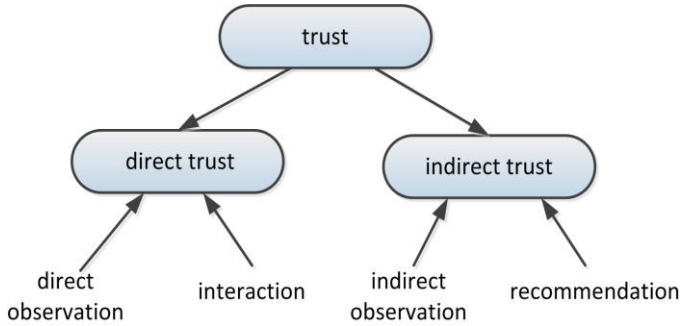

Figure 3. Direct and indirect trust

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.

V. CONCEPT DESCRIPTION

Dynamic evaluation of the environment surrounding the node is possible by continuously monitoring

the node behaviour, with the propsed frame work (Figure 2)

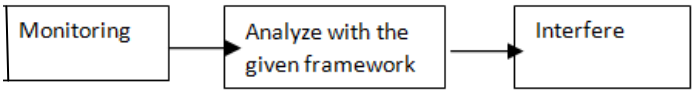

Figure 4. Nodes security evaluation process

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].

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.

VI. 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.

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).
[16] S. Bajpai, A. Sachdeva, J. Gupta, "Security Risk Assessment:Applying the Concept of Fuzzy Logic", *Journal of Hazardous Materials*, Vol. 173, No. 1-3, January 2010, pp.258-264.doi:10.1016/j.jhazmat.2009.08.078
[17] A. Veiga, J. Eloff, "A Framework and Assessment for Information Security Culture", *Computer and Security,*Vol. 29, No. 2, March 2010, pp. 196-207.doi:10.1016/j.cose.2009.09.002
[18] Zakaria I. Saleh, Heba Refai, Ahmad Mashhour "Proposed Framework for Security Risk Assessment" *Journal of Information Security*, 2011, 2, 85-90
[19] tameem eissa, shukor abd razak, md asri ngadi "*Enhancing MANET Security using Secret Public Keys"* 2009 International Conference on Future Networks
[20] Joanna Głowacka, Marek Amanowicz " Application of Dezert-Smarandache Theory for Tactical MANET Security Enhancement"