NEW INNOVATION METHOD FOR SECURE COMMUNICATION BY WIRELESS SENSOR NETWORKS

Irma Aslanishvili

Abstract: *A sensor is a device that detects events or changes in quantities and provides a corresponding output, generally as an electrical or optical signal. The sensor has to do the following tasks: Give a digital signal, be able to communicate the signal, be able to execute logical functions and instructions. Sensors are used in everyday and they are in everywhere in our life. The objective of "new innovation Method to Secure communication for Wireless Sensor Networks" is to provide a collection of high-quality research papers in signal processing for Computer sensor systems and Computer Sensor Networks. This innovation Method motivated by the idea of developing the high effective sensory systems for monitoring of environmental pollution.*

Keywords: *Sensor Networks, Wireless, Modeling and Analysis, MANET protocols.*

Introduction

We study the innovation method for Wireless networks node and our problem of selecting an optimal route in terms of path availability. We propose an approach to improve the efficiency of reactive routing protocols. Ad hoc networks each node acts as a router for other nodes. The traditional link-state and distance-vector algorithms do not scale well in large MANETs.[Namicheishvili et al, 2011]

New innovative method for Wireless sensor networks are more popular. We investigate the following important problems for the wireless ad hoc environment. We address the problem of group access control for secure group communications in ad hoc networks. Wireless Ad Hoc and Sensor Networks envisioned being self-organized, self-healing and autonomous networks, deployed when no fixed infrastructure is either feasible or cost effective. However, the successful commercialization of such networks depends on the implementation of secure network services, for supporting secure applications. Compared to the existing approaches for infrastructure-based networks, we show that in the ad hoc case, the network topology must take into account in the design of a resource-efficient key management schemes. To conserve energy, we incorporate the node location, the "power proximity" between nodes, the path loss characteristics of the medium and the routing topology, in the key management scheme design. While ad hoc networks offer significant advantages in terms of flexibility and cost, they pose great challenges in realizing secure communications via attack-resistant network functions. Oftentimes, ad hoc networks operate untethered in hostile environments in which case, an

adversary may eaves drop communications, attempt to inject false messages into the network, impersonate valid network nodes, or compromise nodes causing them to misbehave. Given that ad hoc networks rely on the cooperation principle, attacks on even a few network nodes can have a significant impact in the overall network performance. Problem Statement Method for New innovative methods to secure communication and distribution of Sensor networks.[Aslanishvili 2012]

We study the problem of enabling nodes of an ad hoc network to determine their location even in the presence of malicious adversaries. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental condition, and by cooperatively pass their data through the network to a main location. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. On the other hand, we can distinguish also two kinds of nodes: Aggregator and Device or Sensor/Actuator.

Area monitoring is a common application of WSNs. In area monitoring, the WSN deployed over a sensor field where some phenomenon is to monitor. When the sensors detect the event being to by monitored, the event reported to one of the base stations, which then takes appropriate action. Sensor nodes can by imagined as small computers, extremely basic in terms of their interfaces and their components.

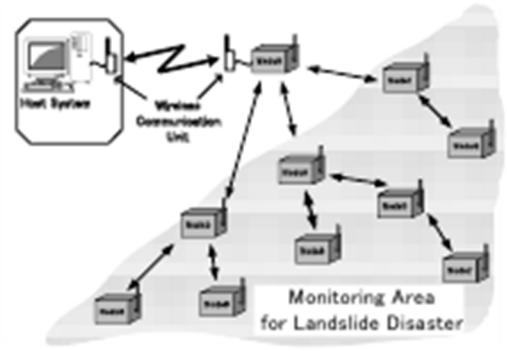

Fig.1 Example of wireless sensory network

This problem will be referred to as Secure Localization. We consider secure localization in the context of the following design goal decentralized implementation, resource efficiency, range-independence, robustness against security threats. Network Model We assume a two-tier network architecture with a set of nodes S of unknown location randomly deployed with a density $q_s$within an area A and a set of specially equipped nodes L we call locators, with known location and orientation, also randomly deployed with a density L << q_s System parametersSince both locators and network nodes are randomly and independently deployed. [Aslanishvili et al 2013] It is essential to select the system parameters, so that locators can communicate with the network nodes. The random deployment of the nodes with a density, is equivalent to a random sampling of the area A with rate P_s. Making use of Spatial Statistics theory, if LHs denotes the set of locators heard by a node s, i.e. being within range R from s, the probability that s hears exactly k locators, given that the locators are randomly and

independently deployed, given by the Poisson distribution: If a node receives a beacon transmitted at a specific antenna sector of a locator Li, it has to be included within that sector. Given the locator-to-node communication range R, the coordinates of the transmitting locators and the sector boundary lines provided by the beacons, each node determine its location as the center of gravity (CoG) of the overlapping region of the different sectors.

The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. The algorithmic approach to modeling, simulating and analyzing WSNs differentiates itself from the protocol approach by the fact that the idealized mathematical models used are more general and easier to analyze.

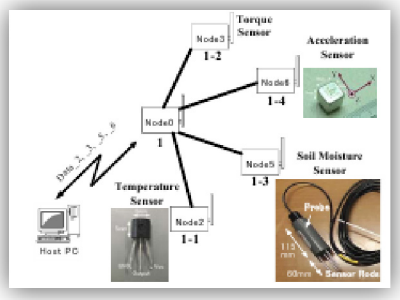

Fig. 2 A simple sensor network for measuring the necessary Parameters.

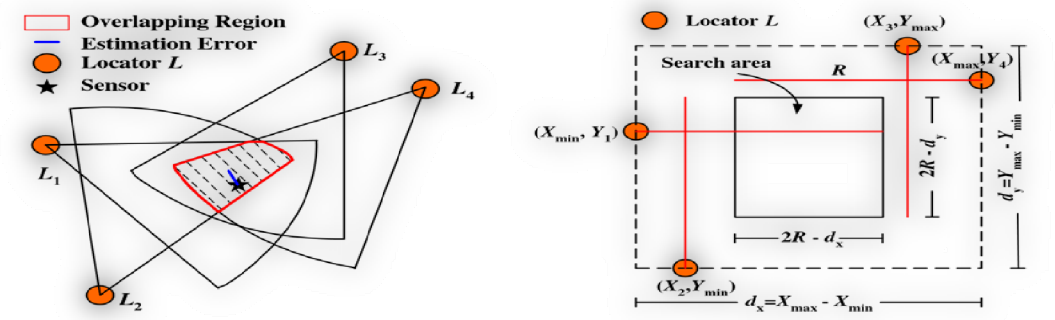

Fig 3. The node hears locators $L_1 \sim L_4$ and estimates its location as the Center of Gravity CoG of the overlapping region of the sectors that include it.

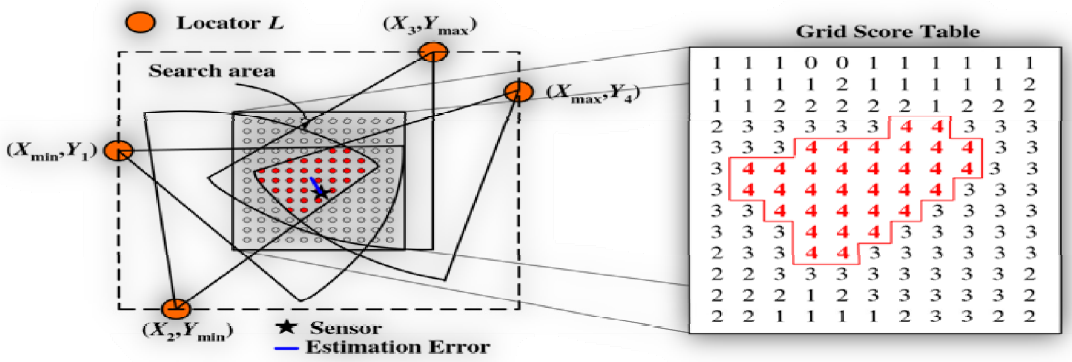

Fig4. The dimensions of the rectangular search area are (2R − d_x)x(2R − d_y) where d_x,d_y are the horizontal distance $d_x = X_{max} - X_{min} \leq 2R$.

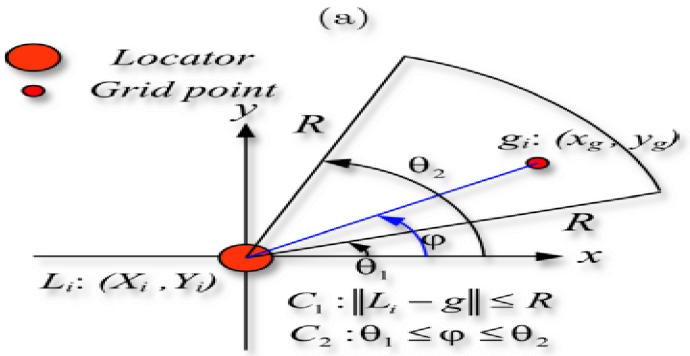

Fig 5. Grid-sector test for a point g

The node estimates its position as the centroid of all grid points with the highest score, [Aslanishvili, 2014] Grid-sector test for a point g of the search area The wormhole attack method - To mount a wormhole attack, an attacker initially establishes a direct link referred as wormhole link between two points in the network. Once the wormhole link is established, the attacker eavesdrops messages at one end of the link, referred as the origin point, tunnels them through the wormhole link and replays them at the other end, referred as the destination The wormhole attack is very difficult to detect, since it is launched without compromising any host, or the integrity and authenticity of the communication.

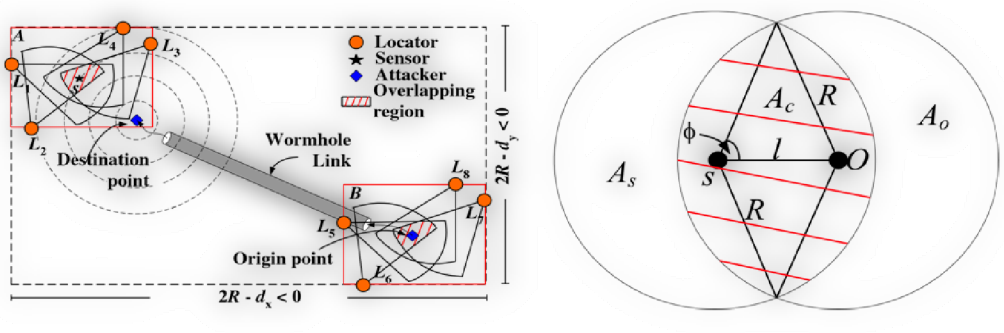

Fig 6. Times its position as the centroid of all grid points with the highest score.

Times its position as the centroid of all grid points with the highest score, Grg of the search are and require each node to frequently recharge its power supply. To overcome the problems associated with the link-state and distance-vector algo-rhythm's a number of routing protocols has been proposed for MANETs. These protocols can be classified into three different groups: proactive, reactive and hybrid. In proactive routing protocols, the routes to all destinations are determined at the start up, and maintained by means of periodic route. [Aslanishvili et al 2015]

Conclusion

New innovation method for Secure communication networks was motivated by the idea of developing the high effective sensory systems for monitoring of environmental pollution, mainly in harsh polluted areas, which can be realized by continuously collecting sensory data from a wireless mobile sensor network deployed in the field. To overcome the problems associated with the link-state and distance-vector algo-rhythm's number of routing protocols have been proposed for MANETs. The relevance of problems particularly pointed out by the environmental dynamism of the shape of fitness function of landscape, which consists of a number of peaks changing width and height in diffuse processes.

Bibliography

[Namicheishvili et al, 2011] Oleg Namicheishvili, Hamlet Meladze, Irma Aslanishvili, Transactions, "Two models for two-hop relay Routing with limited Packet Lifetime", Georgian Technical University, Automated Control Systems, 2011, No1(10), pp. 54-58.

[Aslanishvili, 2012] Irma Aslanishvili, One model for two-hop relay Routing with limited Packet Lifetime the Conference for International Synergy in Energy, Environment, Tourism and contribution of Information Technology in Science, Economy, Society and Education era-7, 2012, ISSN 1791-1133, http://era.teipir.gr

[Aslanishvili ,et al 2013] Energy aware routing model for Wireless and Sensor networks.eRA-8. The contribution of Information Technology to Science, Economy, Society and Education, T.E.I. of Piraeus, Greek; 2013;

[Aslanishvili,et al 2014] Irma Aslanishvili, Three RD Models for Two-Hop Relay Routing With Limited Packets Lifetime In Ad Hoc Networks", International Journal "Information Models and Analyses" Volume 3, Number 3, 2014

[Aslanishvili et al, 2015] Irma Aslanishvili, Paata Kervalishvili, P.Yannakopoulos Novel Methods of Secure Communication and Distribution of Sensor Network https://ener2i.eu/object/event/63/attach/Energy_Innovation_Workshop_2_June_2015_Agenda_ENG_v13a.pdf

Authors' Information

Irma Aslanishvili *– Iv.Javakhishvili Tbilisi State University, Faculty of Exact and Natural Sciences, teacher of Informatics and Computer Sensor Networks; e-mail: Irma.aslanishvili@tsu.ge*

Scientific Research*: General theoretical information research, information systems and computer sensor networks*