CREATING UBIQUITOUS INTELLIGENT SENSING ENVIRONMENTS (CRUISE)

Neeli R. Prasad and Ramjee Prasad
Center for TeleInFrastructure (CTIF), Aalborg University, Denmark

Keywords: CRUISE, Environment, Intelligent Sensing, Applications, Mobility, Security.

Abstract: The recent developments in the research and the technology have brought attention to the wireless sensor networks as one of the key enabling technologies in the next 10 years. Ubiquitous Intelligent Sensing Environments have promising future in supporting the everyday life of the European citizens, bringing important social benefits for each person and for the society as a whole. Taking into account the current fragmentation in the European research in this field, CRUISE Network of Excellence (NoE) intends to be a focal point in the coordination of research on communication and application aspects of wireless sensor networking in Europe. To make a significant contribution to the effectiveness of research, the consortium will evaluate, update and communicate the State-of-the-Art in wireless sensor networking (WSN) to the technical community, distilling a path from current technological status to a long term vision. This paper gives an overview of different research topics in WSN and its open issues.

1 INTRODUCTION

In the past years, a number of mostly U.S.-based research projects (Kahn et al., 1999) depicted WSNs as large-scale networks of homogeneous, tiny, resource-constraint sensor units. While this characterization is valid for large class of applications, an increasing number of sensor network (SN) applications which are envisaged to have immense social benefits for each European citizen and for the society as a whole will play a profound role in the future Ubiquitous Intelligent Sensing Environments. WSNs in vehicles, smart homes, smart offices, applications for road and traffic safety, for emergency response, health monitoring of humans, support for elder people, monitoring of farm animals, etc are mentioned in the literature (Prasad et al., 2004) (Arampatzis et al., 2005) (Konrad Lorincz et al., 2004) (Anu Bhargava et al., 2003). This big diversity of applications requires different design considerations and considerable multidisciplinary research efforts in the areas of communications, electronics, control and close collaboration between users, application domain experts and developers.

The potential for innovative user-centric applications as one of the most exciting aspects of WSN creates a high motivation for working on the variety of challenging research topics (Arampatzis et al., 2005).

In this respect, better coordination for the mostly isolated and disconnected research activities on sensor networks across Europe is essential.

CRUISE (CRUISE, see ref.) Network of Excellence - CReating Ubiquitous Intelligent Sensing Environments, is the new project that deals with WSNs. It actively works against this trend by promoting discussion and strengthening research cooperation and coordination between industry and academia in the topic of communication and application aspects of WSNs, while maintaining its academic nature.

The project starts on 1st January 2006 and has duration of 24 months. 32 internationally recognized groups from Europe, from academia, from independent research centers and from industry, are coordinated by the Center for Telenfrastruktur (CTIF) at Aalborg University, Denmark.

Convinced that Network of Excellence in this field is a necessity in this moment, the project partners share the vision of the ubiquitous intelligent sensing environments and work to reduce the current weakness and fragmentation in this research field in Europe taking into account the immense benefits that WSNs have to offer to the European society.

R. Prasad N. and Prasad R. (2006).
CREATING UBIQUITOUS INTELLIGENT SENSING ENVIRONMENTS (CRUISE).
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 355-361

The jointly executed program of project activities has 3 major directions – integration of knowledge and tools; joint research activities and spreading the excellence.
The main focus is the creation of a state-of-the-art Knowledge Base, available to the European society and the general public, through information and data collection, comparison, validation and then dissemination. To support the research agenda of 6th and 7th Framework Program of the European Commission, CRUISE consortium contributes with identification of the research gaps in the current research work in all fields related to WSNs; with creation of visionary scenarios for future applications of WSNs; with identification of short and long term benefits, done by stimulation of open discussions on the issues of standardization and international collaboration, by broadening the collaboration with industries and the European research initiatives active in this field,. CRUISE partners are to establish frameworks of common tools and methodologies to accelerate the research processes and to build sustainable collaboration links bringing strong commitments to be integrated within and beyond the boundaries of the consortium.
An important aspect of CRUISE potential impact is the new contribution to teaching and training in the field of WSNs. E-learning@CRUISE is the ultimate goal in promoting the research in Wireless Sensor Network and in the spreading of the results to the general public and in particular to the European industry so that it can compete in this domain.
The project consortium is consulted by External advisory board (EAB) on international developments especially desires for (new) actions, projects and activities in the area of wireless sensor networks and applications. EAB consist of international experts in the field of WSNs from all over the world (USA, Turkey, Canada, Australia, Japan, The Netherlands, UK, Switzerland, Portugal), from industry and academia.
This paper is organized as follows: section II provides overview of the Applications and scenarios; section III discussed the mobility in WSN, section IV gives the insight of security issues in WSN and finally the paper is concluded in section V.

2 CRUISE APPLICATIONS AND SCENARIOS

Within the next few years, distributed sensing and computing will be everywhere, i.e., homes, offices, factories, automobiles, shopping centers, supermarkets, farms, forests, rivers, lakes, and even pockets.
Some of the immediate commercial applications of WSN are

- Industrial automation (process control)
- Environmental (ecology system monitoring)
- Defense (unattended sensors, real-time monitoring)
- Utilities (automated meter reading),
- Weather prediction (temperature, humidity)
- Security (smart building, tracking, car theft detecting)
- Building automation (HVAC controllers).
- Disaster relief operations (earthquake, firefighting)
- Medical monitoring and instrumentation (remote sensing and health care)
- Intelligent transportation (unmanned driving)

Research Challenges

- Numerous unattended and resource-constrained sensors, deployed at high density in regions requiring surveillance and monitoring. Network topology is unknown due to unexpected node failures.
- Sensors are memory as well as energy constrained, and power consumption in WSN can be divided into three domains:
- Communication, Data Processing, and Sensing
- A sensor expends maximum energy in data communication (both for transmission and reception), and the transceiver circuitry has both active and start-up power consumption.
- Power consumption in data processing is much less than in communication, so local data processing is crucial in minimizing power consumption in a multi-hop network.
- Tradeoff between energy and QoS
- Prolong network lifetime by sacrificing application requirements, such as delay, throughput, reliability, data fidelity.

3 MOBILITY

The existing state-of-the-art can be organized, on one hand, into the analysis of different sensors,

depending on the application and on the other hand, the processing algorithms involved taking into account the constrains of the devices (motes), the monitoring process and the trade-off between delay and throughput.

For the targeted applications, environmental monitoring and road traffic monitoring, we have different approaches in the state-of-the-art. For environmental monitoring: U.S. NSF (US NSF, see ref.) , DARPA (DARPA, see ref.) and INTEL (INTEL, see ref.) , in U.S.; IBM Zurich (IBM , see ref), EPFL (MICS, see ref.) in Switzerland; Australian Research Council (Australian Research Council, see ref.) and for road traffic monitoring: Pravin Varaiya's Group (Berkeley) (Pravin Varaiya's Group, see ref.) and Cartel People (MIT) (Cartel People (MIT), see ref.).

Different sources of mobility are:

- Node mobility
  - A node participating as source/sink (or destination) or a relay node might move around
  - Deliberately, self-propelled or by external force; targeted or at random
  - Happens in both WSN and MANET
- Sink mobility
  - In WSN, a sink that is not part of the WSN might move
  - Mobile requester
- Event mobility
  - In WSN, event that is to be observed moves around (or extends, shrinks)
  - Different WSN nodes become "responsible" for surveillance of such an event

The processing algorithms to optimize sensors in environment application and scenario within the WSN framework can be determined by the objective of these applications such as:

For environmental monitoring:

- Watershed and quality water monitoring, where data is used to: a) analyze the effect of pollution in water and soil conditions, b) track groundwater flows
- Early detection of forest fires, where WSNs will include temperature, light, soil moisture and air humidity sensors to estimate evaporation, as well as sensors to measure wind speed and direction, allowing inferring fire risk levels and probable fire direction.

For road traffic monitoring:

- Vehicle tracking, detection and classification (e.g. length, speed, etc.), using acoustic, magnetic and infrared sensors and tiny cameras
- Intelligent & efficient parking on public streets, finding free parking spots for drivers, decreasing the risk of possible accidents and pollution

Mobility can be described along two-axis: *location* coordinate and *time*

- Mobile enabled WSN will provide *time-varying* topological view to task managers
- Mobility maybe can be leveraged to realize the "*divide and conquer*" idea, i.e. not acting until appropriate opportunity
- Mobility management in WSN requires *nano*-scale location management and topology management

Sensor relocation can assist the deployment of sensor network to meet certain *coverage* requirement. Sensor mobility provides a *time-varying* coverage that is of benefit to monitor moving intrusion target. Mobile sink can collect information from vicinal sensors and *make decision* about its mobility pattern. The sink's mobility pattern can be *learned* and leveraged by sensors to dynamically choose best route and finally, mobile *relay* is another alternative to alleviate the burden of energy consumption bottleneck of the sensor nodes around the sink.

4 SECURITY

When designing a secure WSN, the following security requirements should be considered: authentication, integrity, freshness, availability, confidentiality, robustness, autonomous recovery, privacy protection, trust establishment. In the following paragraphs, state-of-the-art for each of them is provided and open research issues are identified.

Authentication:

The broadcast nature of the transmission medium makes information more vulnerable than in wired applications. Thus, security mechanisms such as encryption and authentication are essential to protect information transfers.

Key management protocol:

Symmetric encryption/decryption algorithms and hashing functions are between two to four orders of magnitude faster than Public-key algorithms, such as RSA, and constitute the basic tools for securing sensor networks communications.

In (Tassos Dimitriou et al., 2005) a localized algorithm for key establishment between a source node and the base station suitable for sensor network deployment is proposed. The protocol provides

security against a large number of attacks and guarantees that data securely reaches the base station in an energy efficient manner.

Encryption algorithms:

TEA, SEAL, RC4, RC5 (Xiaohua Luo et al., 2004).These encryption algorithms are suitable for sensor networks with harsh resource constraints. According to the comparison performed in (Xiaohua Luo et al., 2004). TEA is the most perfect encryption algorithm to minimize memory footprint and maximize speed. Disadvantage of SEAL - it requires several kilobytes of RAM space and rather intensive computation.

RC4 is widely used in many applications and is generally regarded to be secure.

µTesla (John Kelsey et al., 1997): Broadcast authentication is a critical security service in sensor networks; it allows a sender to broadcast messages to multiple nodes in an authenticated way. µTESLA and multi-level µTESLA have been proposed to provide such services for sensor networks. The propose approach removes the authentication delay as well as the vulnerability to DOS attacks during the distribution of µTESLA parameters, and at the same time allows a large number of senders but requires loosely time synchronization between senders and receivers.

Integrity:

The danger is that information could be altered when exchanged over insecure networks. An attacker can perform a wide variety of attacks (once the attacker compromised the base station or the aggregators, the attacker could perform a denial-of-service attack and stop responding to any queries). Since it is assumed that a compromised node is under the full control of the attacker, there is nothing to prevent the attacker from mounting such denial-of-service attacks.

The approach introduced in (Bartosz Przydatek et al., 2004) against stealthy attack is for of *secure* information aggregation in sensor networks, with analysis of the attack model and security requirements. It proposes the *aggregate-commit-prove* framework for designing secure information aggregation protocols; proposes the approach of *forward secure authentication* to ensure that even if an attacker corrupts a sensor node at a point in time, it will not be able to change any previous readings the sensor has recorded locally.

Freshness:

Verifying physical presence of a neighbor in wireless networks is one of the key components in developing protocols resilient to replay-based attacks. One of the key issues is how to verify whether the given two neighbors are actually within each other's transmission range or not without increasing the complexity or requiring additional hardware; if this fundamental question can be addressed in an efficient and scalable manner, then the replay-based attacks can easily be determined and eliminated by canceling fake neighboring relations.

The Two methods proposed in (Turgay Korkmaz, 2005) are possible solutions with the objective of increasing the rate of making correct decisions when checking neighboring relations, supporting and justifying the proposed ideas.

Focusing on RTS/CTS patterns in a given neighborhood and analyze them with the objective of detecting physically impossible neighboring relations.

Availability:

In a sensor network many risks can result in a loss of availability such as denial of service attacks etc. In (Wood et al., 2002) a geographic routing protocol for sinkhole and wormholes attack is proposed.

Sinkhole and wormholes attacks: geographic routing protocol - Sensor networks are susceptible to sinkhole attacks because of their specific communication pattern, and also because all packets share the same ultimate destination (in networks with only one base station). Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. The situation becomes worse when the two are used in combination.

One class of protocols resistant to these attacks is geographic routing protocols. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station. Because traffic is naturally routed towards the physical location of a base station, it is difficult to attract it elsewhere to create a sinkhole.

Sybil attack (Karlof et al., 2002) **-** In a Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, and multipath. Sybil attacks also pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets because by using

the sybil attack, an adversary can "be in more than one place at once".

Intrusion and Misbehavior detection:

In sensor networks, many potential sources of faulty packets exist. The source may be benign, such as a malfunctioning sensor reporting impossible data, or the source may be malicious - an outside attacker performing a denial-of-service by injecting garbage data, or a compromised node triggering false alarms or misleading data. As possible solution, Sensor Node Traceback Scheme (SNTS) to trace malicious packets into the network is proposed in (Damon Smith et al., 2004).

As the same time reliable and timely detection of deviation from legitimate protocol operation is recognized as a prerequisite for ensuring efficient use of resources and minimizing performance losses. The basic feature of attack and misbehavior strategies is that they are entirely unpredictable. The random nature of protocol operation together with the inherent difficulty of monitoring in the open and highly volatile wireless medium poses significant challenges.

Resilience to node capture and ensuring Confidentiality:

By using cryptography in the sensors, it is easy to prevent attacks by unauthorized intruders. On the other side, cryptography by itself cannot prevent node capture or inside attackers because in this case the attacker would have the full control over the sensor, including the cryptographic keys.

One-time sensors - In (Kemal Bicakci et al., 2005) the concept of one-time sensors to mitigate node-capture attacks is proposed by utilizing the low-cost property of sensor nodes. The idea is to preload every sensor with a single cryptographic token before deployment, so that any node can only insert one legitimate message. If the sensor is captured, this sensor can only inject a single malicious message in the sensor network.

However this approach is not an appropriate choice for applications that require sensors to send arbitrary messages and the integrity and/or confidentiality of these messages should be protected, in particular dealing with medical care sensors.

Robustness against attacks:

WSN protocols need to be able to identify failed neighbor nodes in real time and to adjust accordingly to the updated topology. At the network level, the routing protocol should be made aware of faulty nodes to ensure that faulty nodes are routed around.

Self diagnosing sensor nodes - A method of introducing a level of fault tolerance into wireless sensor networks is proposed in (Harte et al., 2005), performed by monitoring the hardware and detecting the status of physical malfunctions, caused by impacts or incorrect orientation.

Software analysis is performed on the raw data from the accelerometers to determine the orientation of the node and to detect impacts.

Event boundary detection - The main purpose is to identify the faulty sensors and detection of the reach of events in sensor networks with faulty sensors. Two novel algorithms for faulty sensor identification and fault-tolerant event boundary detection are proposed and analyzed in (Ding et al., 2005). These algorithms are purely localized and thus scale well to large sensor networks. The computational overhead is low, since only simple numerical operations are involved. The algorithms can be applied as long as the "events" can be modeled by numerical numbers.

Modeling and Detection of Misbehavior in WSNs:

The pervasiveness of wireless sensor devices and the architectural organization of wireless sensor networks in distributed communities, where no trust can be assumed, are the main reasons for the growing interest in the issue of compliance to protocol rules. Reliable and timely detection of deviation from legitimate protocol operation is recognized as a prerequisite for ensuring efficient use of resources and minimizing performance losses. The basic feature of attack and misbehavior strategies is that they are entirely unpredictable. In the presence of such uncertainty, it is meaningful to seek models and decision rules that are robust, namely they perform well for a wide range of uncertainty conditions. One useful design philosophy is to identify the rule that optimizes worst-case performance over the class of allowed uncertainty conditions. The situation is challenging because several protocols operate in a non-deterministic manner. Thus the distinction of normal behavior from occasional misbehavior is not straightforward.

In a wireless network, information about the behavior of nodes is available to immediate neighbors through direct observations. If these measurements are compared with their counterparts for normal protocol operation, it is then contingent upon the detection rule to decide whether the protocol is normally executed or not. Furthermore, we propose to study the interaction between the detection system and the attacker as players participating in a zero-sum game. On the one hand, the detection system would like to devise a detection

rule that minimizes detection time of the attacker. On the other hand, the attacker would like to behave so as to prolong detection as much as possible. Therefore, the objective function in that aspect would be detection time.

5 CONCLUSIONS

The CRUISE project marks the start of a long-term research and education co-operation initiative among leading European universities and research institutes in the field of wireless sensor networks and applications. The results of CRUISE will be available to interested European research organizations, industry, SMEs and to the wide public.

Wireless sensor networks are a reality. The market for ZigBee devices, including smart dust, will grow to 150 million units by 2008 creating a billion dollar business. Much research has been done. TinyOS is a good research platform, but not an industry strength software.

WSNs need killer application. It is not clear what the killer application is. But certainly environment monitoring is not.

Nomadic user based WSN routing and Mobile WSNs represent new challenges to do research and development in this exciting area. Mobility in wireless sensor networks poses unique challenges to the medium access control (MAC) protocol design. Previous MAC protocols for sensor networks assume static sensor nodes and focus on energy efficiency.

ACKNOWLEDGEMENTS

This work has been performed in the framework of the IST-4-027738 NoE CRUISE, which is partly funded by the European Union. The authors would like to acknowledge the contribution of their colleagues from the consortium.

REFERENCES

J.M. Kahn, R.H. Katz, and K.S.J. Pister. Mobile networking for “Smart Dust”. Proceedings of IEEE/ACM Mobile Computing and Networking Conference (Mobicom '99), August 1999

N. R. Prasad and M. Ruggieri, “Adaptive security for Low Data Rate networks,” Special Issue on Security, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, 2004

Th. Arampatzis, J. Lygeros, A Survey of Applications of Wireless Sensors and Wireless Sensor Networks, Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005, pp719-724

Konrad Lorincz, David J. Malan, et al, Sensor Networks for Emergency Response: Challenges and Opportunities, PERVASIVE computing Published by the IEEE CS and IEEE ComSoc – 2004

Anu Bhargava and Mike Zoltowski, Sensors and Wireless Communication for Medical Care, Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA’03), IEEE - Computer Society 2003

CRUISE project website link: http://www.telecom.ece.ntua.gr/cruise/

US NSF Center for Embedded Networking Sensing (CENS), UCLA, http://www.cens.ucla.edu/

DARPA Grant, CoSense, http://www2.parc.com/spl/projects/cosense/ , Palo Alto Research.

INTEL Research, Sensor Nets, http://www.intel.com/research/exploratory/wireless_sensors.htm

IBM Zurich, Sensor Networks, http://www.zurich.ibm.com/sys/communication/sensors.html

MICS (Mobile Information and Communication Systems) SNSF project, http://www.mics.ch

Australian Research Council, Sensor Networks, http://www.sensornetworks.net.au/

Pravin Varaiya’s Group. Electrical Engineering and Computer Science University of California, Berkeley, CA, http://path.berkeley.edu/~singyiu/vehicledetection/main/main.htm

Cartel People (MIT) http://cartel.csail.mit.edu/

Tassos Dimitriou, I. Krontiris and F. Nikakis. “A Localized, Distributed Protocol for Secure Information Exchange in Sensor Networks”. 5th IEEE International Workshop on. Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks, WMAN 05.

Xiaohua Luo; Kougen Zheng; Yunhe Pan; Zhaohui Wu; Encryption algorithms comparisons for wireless networked sensors, Systems, Man and Cybernetics, 2004 IEEE International Conference on Volume 2, 10-13 Oct. 2004 Page(s):1142 - 1146 vol.2

John Kelsey, Bruce Schneier, David Wagner, Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA, ICICS, 1997, pages 233-246

Bartosz Przydatek, Dawn Song, and Adrian Perrig. *SIA: Secure Information Aggregation in Sensor Networks*. In Proc. of the 2nd ACM Conference on Embedded Network Sensor Systems (SenSys), Los Angeles, CA, USA, November 2004.

Turgay Korkmaz, Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless

Ad Hoc Networks, International Journal of Information Technology (IJIT), Volume 11 Number 2, 2005, pages 5-17

Wood, A. D., and Stankovic, J. A. *Denial of service in sensor networks*. IEEE Computer. , 2002, p. 54-62

C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in IEEE SPNA, 2002.

Damon Smith, Ryan Mahon, Swathi Koundinya, Shubhashri Panicker. SNTS: Sensor Node Traceback Scheme. ACM WiSe 2004, October 1, 2004.

Kemal Bicakci, Chandana Gamage, Bruno Crispo, and Andrew Tanenbaum, *One-Time Sensors: A Novel Concept to Mitigate Node-Capture Attacks*, ESAS2005: 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, 2005.

Harte, S.; Rahman, A.; Razeeb, K.M.; Fault Tolerance in Sensor Networks Using Self- Diagnosing Sensor Nodes, The IEE International Workshop on Intelligent Environments, 2005. (Ref. No. 2005/11059), 29 June 2005 Page(s):7 – 12

Ding, M.; Chen, D.; Xing, K.; Cheng, X.; Localized Fault-Tolerant Event Boundary Detection in Sensor Networks, INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, Volume 2, 13-17 March 2005 Page(s):902 - 913 vol. 2