Trustworthy Sensor Networks: Issues, Challenges & Solutions

Saurabh Ganeriwal and Mani B. Srivastava
Networked and Embedded Systems lab
56-125B, EE-IV, University of California Los Angeles
{saurabh, mani}@ee.ucla.edu

Abstract

Building sensor networks poses challenges of secure routing, node authentication, data integrity, data confidentiality and access control that are faced in conventional wireless and wired networks as well. In this paper, we argue that the conventional view of security based on cryptography and authentication alone is not sufficient for the unique characteristics and novel misbehaviors encountered in sensor networks. Fundamental to this is the observation that sensor network applications are based on collective interaction between a large numbers of nodes, which do collaborative data gathering, collective data/information processing, and multi-hop data delivery. This decentralized in-network decision-making, which relies on the inherent trust among the sensor nodes, can be abused by adversaries to carry out security breaches. An adversary can potentially insert bogus data to mislead the whole network! Cryptographic mechanisms alone cannot be used to solve this problem as adversarial or faulty sensor nodes can use valid cryptographic keys to authenticate bogus data.

We highlight some scenarios where solely using cryptography fails. On the basis of these observations, we motivate the need of integrating tools from different domains such as economics, statistics and data analysis with cryptography to facilitate the development of high integrity sensor networks. Following this approach, we introduce a reputation-based framework that provides a unified solution for countering several types of malicious/non-malicious misbehavior in sensor networks.

1. Introduction

The traditional approach of providing network security has been to borrow tools from cryptography and authentication[1]. In general, cryptography based schemes aim at providing data confidentiality, data integrity, node authentication, secure routing and access control. However, unlike traditional ad-hoc wireless networks, cryptography by itself cannot provide a complete solution to developing trustworthy sensor networks.

A major distinction that sets sensor networks apart from traditional ad-hoc networks is that security breach can happen in a sensor network not only while relaying information to the end-user but also while generating information. The ability of a sensor network to perform its task depends not only on its ability to communicate among the nodes, but also on its ability to sense the physical environment and collectively process the sensed data. This decentralized in-network decision-making, which relies on the inherent trust among the sensor nodes, can be abused by adversaries to carry out security breaches through compromised nodes. Note that sensor nodes are envisioned to be low-cost which make it infeasible for manufactures to make them tamper-resistant; an adversary can undetectably take the control of a sensor node by physically compromising it. An adversary can then potentially insert faulty data or information to mislead the whole network! Clearly, cryptographic mechanisms alone cannot be used to solve this problem as internal adversarial nodes will have access to valid cryptographic keys and they can use these keys to authenticate bogus data. Besides malicious attacks, the two other system characteristics that hinder the development of high integrity sensor networks are *system faults* and *sensing channel inconsistencies*. Sensor nodes are currently made of cheap hardware components, highly vulnerable to system malfunctioning. Non-malicious behavior such as malfunctioning of radios/sensors can also result in the generation of bogus data, bringing equally detrimental effects to the functioning of the network. Another distinguishing trait of sensor networks is their strong coupling with the physical world. This gives rise to a unique opportunity for adversaries, whereby instead of abusing the network, they can insert bogus data into the network by abusing the physical world. The very nature of this type of misbehavior is outside the realm of cryptography.

We believe that in general solutions for developing trustworthy sensor networks will encompass tools from different domains such as economics, statistics, data analysis and of course cryptography. Based on this observation, we are currently exploring an approach motivated from existing human societies in the world. Embedded in every social network is a web of *trust;* with a link representing the trustworthiness between two individuals. When faced with uncertainty, individuals seek the opinions of those they trust. The intent is to develop a similar Reputation-based Framework for Sensor Networks (RFSN), where sensor nodes maintain *reputation* for other nodes and use it to evaluate their trustworthiness. We will analyze the features of RFSN in detail, making a

[1] Referred as cryptography throughout the paper.

compelling case to develop such systems. We conclude the paper outlining challenges for the realization of RFSN and propose agendas for future research to achieve high integrity sensor networks.

2. Secure Sensor Network Challenges

A. Secure Communication

Sensor networks mostly operate on wireless communication medium which is difficult to constrain; it is by nature a broadcast medium where adversaries can easily eavesdrop on, intercept, inject, and alter transmitted data. In [1], authors do a detailed study on the resiliency of existing routing protocols in the presence of malicious attacks such as denial to forward packets, unnecessary flooding of packets, black hole attacks, wormholes etc [2]. They conclude that most of the protocols breakdown as they were not designed keeping security into mind, highlighting the limitations of existing routing approaches in sensor networks. Moreover, these devices have limited computational power, memory, communication bandwidth, and energy resources which restrict the portability of existing security mechanisms. Having realized this inadequacy, several cryptographic schemes have been proposed such as SPINS [3], TinySec[4], μ-TESLA[3], INSENS [5] that aim at providing data confidentiality, data integrity, node authentication, secure routing and access control. The establishment and management of cryptographic keys [3, 6, 7, 8, 9] forms the backbone of these schemes; the scale and ad-hoc deployment of nodes coupled with the ability of adversaries to easily recover the cryptographic materials make it a challenging problem to solve. In [10], authors highlight several key challenges and lay down future directions for cryptographic research. We argue that cryptography presents an efficient mechanism but not a complete solution for the novel misbehaviors encountered in sensor networks. We highlight this in the forthcoming subsections by introducing new classes of challenges for realizing trustworthy sensor networks.

B. Collaborative Data Processing

Instead of providing a raw dump of sensor data, sensor networks often use in-network processing algorithms (aggregation) that besides saving energy also provide meaningful results to the end user. Similarly, sense-response applications such as fire monitoring and target tracking rely on decentralized decision making by a population of nodes. An inherent assumption is that all nodes will abide by the rules of the protocol. However, sensor nodes are envisioned to cheap and therefore unlikely to be equipped with tamper-proof hardware. This coupled with the unattended operation of these networks leaves the node at the mercy of an adversary who can potentially steal nodes, recover their cryptographic material, and pose as an authorized node in the network. Thereafter, these internal adversaries can exploit the inherent trust between the nodes to abuse the functioning of these protocols.

To emphasize our point we present an example in Figure 1, depicting a sensor network deployed for intrusion detection. When a target is detected at (x, y), the normal behavior of the network will be the following – Node C will collect the raw sensor data from A and B, it will fuse this information with its own reading to find the target's location and will eventually report this location to the end user using a multihop route through D, E, F and G. If an attacker compromises C, it can either hide the identity of the intrusion by not sending the processed results or can even mislead the user by reporting a false location estimate of the intruder, (w, z) instead of the real position (x, y).

Only recently some proposals have been proposed to counter or restrict the impact of these attacks, SIA[11], SERP[9], SEF[12] etc., which use the scale and redundancy in the system to their advantage. In general, cryptography alone cannot solve this problem as adversaries can generate bogus information and still authenticate it using valid cryptographic keys.

C. Data Authentication

Sensor network applications not only rely on the ability of nodes to communicate among themselves but also on their ability to sense the physical environment. However, internal adversaries after compromising a node (or its transducer) can insert bogus data, thereby misleading the whole network. For example, if an attacker compromises A or B (Figure 1), it can send false information "Target detected at (w, z)"; thereby making it hard for C to conclude anything about the intruder location. Note that data authentication is different from data integrity. Attaching message authentication codes can verify the consistency of data but cannot verify its validity as the source generating the data itself can be malicious. Cryptographic solutions will be again limited by the fact that adversaries have access to valid keys.

Faulty nodes: Besides malicious security breaches, bogus data can also be generated by nodes unintentionally due to the failure of some system components such as radio/sensors etc. For example a temperature sensor might be producing wrong reading if mud falls on it. Sensor nodes are made of cheap hardware components which are highly vulnerable to system malfunctioning. We expect the network designers to leverage Moore's law to drive down power consumption and cost even more instead of increasing robustness as power and cost continue to be major deployment bottlenecks.

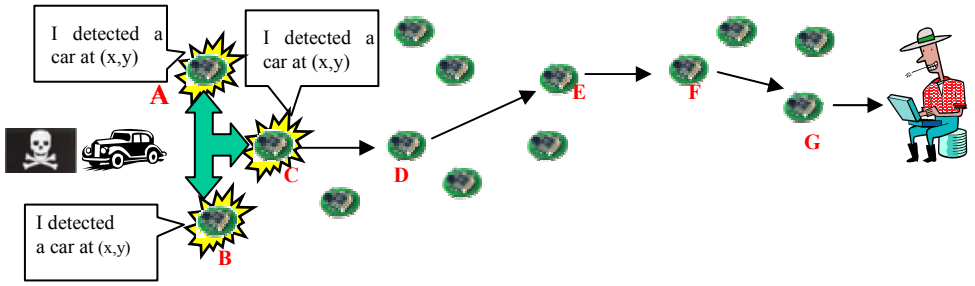

Figure 1. **Sensor Network deployed for intrusion detection**

However, whether a node produces a wrong reading either after being compromised or due to system failure, both are equally detrimental to the functioning of the network. Security mechanisms developed using cryptographic techniques will not differentiate between readings from faulty and good sensor nodes, resulting into inaccurate results. Cryptography concentrates on providing resiliency against security breaches and such non-malicious activity has to be handled borrowing tools from other domains.

D. Malicious Environment

A distinguishing trait of sensor networks is their strong coupling with the physical world. It is important to realize that the user is not interested in values from a group of sensor nodes but is instead trying to learn some parameters of the underlying physical process. This gives rise to a unique opportunity for adversaries, whereby instead of abusing the network, they can bring equally detrimental effects by abusing the physical world. An example attack is the malicious insertion of a heat source in a sensor network deployed for monitoring temperature. The abuse of the physical world results in the same problem of data authentication; albeit its nature is entirely different. In this scenario, adversary is not a physical entity (sensor node) but the whole physical world. Cryptography provides tools for securing the system and cannot be used to provide countermeasures against process-centric attacks.

3. Reputation-based Framework (RFSN)

In ad-hoc networks a malicious node can alter the information only if other nodes in the network choose the malicious node to act as a relay. However, in sensor networks besides the above attack a malicious user can also harm the system at the stage when the information is generated either at the stage of data processing or data generation.

A. Motivation

The problem of generating reliable information in sensor networks can be reduced to one basic question – How do sensor nodes trust each other? We take the motivation from observing the evolution of existing social networks in the world. Embedded in every social network is a web of trust with a link representing the amount of trust between two individuals [13]. Let's try to analyze the integrated role of "reputation" and "trust" in these networks. *Trust* can simply be defined as the expectation of one person about the actions of others. It is used by the first person to make a choice, when an action must be taken before the actions of others are known. *Reputation* is defined as the perception that a person has of another's intentions. When facing uncertainty, individuals tend to trust those which have a reputation for being trustworthy.

RFSN is a similar framework where sensor nodes maintain *reputation* for other nodes in the network. A node monitors the behavior of other nodes, based on which it builds up this reputation over time. It uses this reputation to evaluate the trustworthiness and in predicting the future behavior of different nodes. At the time of collaboration, a node only cooperates with those nodes that it trusts. The end objective of RFSN is to generate a community of trustworthy sensor nodes. In a community model, members share some common resources and simultaneously contribute to the community life in order to be entitled to use those resources. In our context, sensor nodes are the members of this community. They contribute to the community life by collaborating in meeting the end-user objective. The network resources which they share are each other. Note that the end-user objective can only be met by collaborative data processing between nodes and a sensor node individually cannot provide any meaningful information to the end user. The key to the development of highly reliable sensor networks lie in making the nodes collaborate with only other good (non-malicious and non-faulty) in the network. Using RFSN, nodes with bad reputation, because they are malicious or are faulty, will be excluded from the community. It is important to realize that even malicious attacks are carried out by an attacker after seeking the cooperation (unknowingly) of other non-malicious nodes in the network. Let us revisit the network scenario depicted in Figure 1 to verify this assertion. In this scenario, nodes D, E, F or G can block packet forwarding only if node C chooses the respective compromised node to cooperate by acting as the intermediate relay. Similarly a false negative attack by A or B is possible only if node C takes into account the value reported by node A or B in calculating the final result. Finally, C can harm the system

only if A and B choose C to act as the processing center. A framework based upon reputation and trust will help the nodes to distinguish good nodes from bad, thereby preventing themselves from being exploited by the malicious or failed nodes in the network.

B. Architecture

RFSN runs at the middleware of every sensor node. Figure 2 depicts the key building blocks of RFSN; the direction of the arrow represents the flow of information.

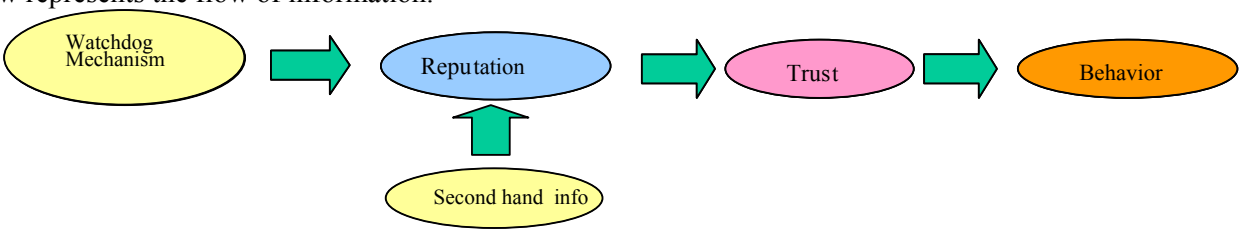

Figure 2. **Architectural Design of RFSN**

This block can be viewed as a collection of discrete modules. Each module carries out a specific function that can range from monitoring communication channel to sensing channel. However, each module also imposes extra resource requirements on the system in terms of energy, storage or processing cost. For example *WMRouting* monitors the data forwarding behavior of the neighboring nodes by keeping the radio active in the promiscuous mode.

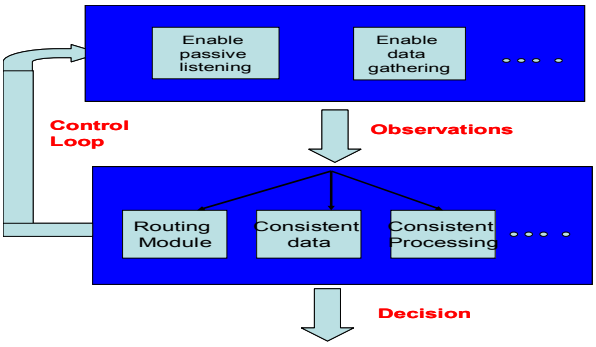

Figure 3. **Watchdog Mechanism**

Reputation: Reputation of a node is maintained as a probabilistic distribution, enabling the node to have full freedom and not get constrained by some discrete levels of reputation (+/-1, 0) as used in eBay [14]. Further, maintaining a statistical representation for reputation is more consistent with the model of RFSN as reputation can only be used to predict the future behavior of other nodes and cannot define deterministically the actual action performed by them.

Second hand information: If a node just relies on its direct observations to build reputation information, the convergence time might be very large. Moreover, these observations will typically impose a huge learning cost. A simple optimization is for nodes to use each others experiences with other nodes in the network. Thus, nodes exchange reputation information and we classify these indirect observations as second hand information.

Watchdog Mechanism: The node classifies the actions performed by other nodes in the network as cooperative or uncooperative. This block is responsible for collecting these observations as well as for making the decision as depicted in Figure 3.

Trust: Trust is a subjective expectation a node has about another node's future behavior. This is obtained by taking the statistical expectation of the probability distribution representing the reputation.

Behavior: When faced with the question of cooperating with a node j in the network, the behavior of node i, B_{ij}, *{cooperate, don't cooperate},* is derived using a simple thresholding on the trust metric between them. Behavior provides a higher-level abstraction; node's actual action will be based on it. We again trace back to the example of Figure 1, where node C has been compromised. If RFSN works perfectly fine, nodes A and B will calculate B_{AC} and B_{BC} to be *don't cooperate* respectively. They will utilize this information to choose some other data processing center that is trustworthy.

4. Analysis of RFSN

A. Why can RFSN work?

Scalability: Most of the sensor network applications are based on local interactions between nodes that typically lie in the broadcast domain of each other. Moreover, these networks are relatively static so that the subset of nodes with which a node interacts remains almost similar throughout the network lifetime. This makes RFSN scalable. Not only it is sufficient for nodes to maintain reputation for only a few nodes but they can establish these metrics though simple local interactions.

Generalized: Several customized solutions, based on cryptography, for providing secure communication, aggregation, data integrity, access control etc. have been developed in the realm of sensor networks. RFSN do not eradicate the need of them; in fact these solutions can be part of the watchdog mechanism as discrete modules. RFSN integrates all of them to provide one classifying

metric, reputation, for a node. Cryptographic schemes such as SERP [9], SIA[11], SPINS [3] etc. can then exploit this reputation information, build using RFSN, to decide the subset of nodes with which to interact while doing key establishment, generating secure event reports etc. in future. Thus, RFSN can work in conjunction with these schemes to provide a complete solution for high integrity sensor networks.

Unified: In RFSN, a sensor node act upon any inconsistent behavior without caring about the origin of it. From a network perspective, both malicious and faulty behavior is equally detrimental and hence, should be acted upon in a similar fashion. Temporary system faults such as temporary malfunctioning of sensor/radio or network faults such as fading on the communication channel will span over a small duration of time and maintaining a probabilistic distribution for reputation will automatically filter out such sporadic behavior. Permanent faults will indeed be dealt in the same manner as malicious nodes.

Diversity: Different applications can be provided with varied security options by setting application specific threshold values for judging the trustworthiness of a node. For example an application that finds the maximum temperature value in a room can have relatively smaller threshold value compared to an intrusion detection application. Furthermore, the requirements of the security level can be also changed at runtime, say after detecting a breach, by runtime update of the threshold.

Selfish Misbehavior: A tricky scenario for reputation-based systems is to handle the selfish misbehavior attacks often seen in the realm of traditional ad-hoc networks. For example, in order to preserve its own battery resource, a node might seek to minimize its use for cooperative behavior. In RFSN, we do not provide any exclusive measures to counter such selfish misbehavior attacks because we believe that these attacks would never take place in sensor networks. It is important to realize that the whole sensor network is a single entity. The survival of a single node is irrelevant and what matters is whether the network is functional or not. Thus, a node never falls in the dilemma of selfish behavior v/s cooperation. A non-malicious node is supposed to cooperate at all the time.

B. Challenges

In this section, we will lay down some of the challenges for realizing RFSN. We also introduce some approaches for handling these issues that we are currently pursuing as a part of developing an example system under the framework of RFSN.

Statistical Formulation: Mathematical tools are needed for reputation representation, updates and integration. Existing reputation based frameworks either assume a deterministic model for representing reputation [14] or portray a very high level picture of the probabilistic framework based on trivial and debatable heuristics [15, 16, 17]. We have developed a concrete Bayesian Formulation, based on beta reputation systems [18], to represent reputation, update it continuously based on new direct/indirect observations and finally, make the transition from reputation to the trust metric of a node.

Watchdog Mechanism: This block helps a node build reputation over time; albeit at the cost of some resources. Therefore, a judicious choice of modules is paramount to the success of RFSN. We are currently investigating existing and novel challenge-response protocols, outlier-detections schemes and data analysis protocols to develop these modules. We envision running this block in a customized manner; modules are available as APIs and it is the responsibility of the end-user to enable a subset of them. Moreover, the system design should allow an easy runtime insertion/removal of these modules.

Bootstrapping: RFSN takes a pessimistic approach at the onset of the network, whereby no node in the network trusts each other. The reputation gradually builds up over time. An inherent assumption made is that there exists significant opportunities in the network whereby nodes can learn about each other. However, there exist sense-response applications where the expected network activity is low. Thus, a mechanism is needed to pro-actively establish trust among nodes. We are pursuing the direction of using mobile trustworthy nodes as a bootstrapping mechanism for trust establishment. These nodes can be used to fabricate some events in the network, thereby providing opportunities for the nodes to monitor each other's behavior.

Hierarchical structure: RFSN operates on the basic principle of Bayesian decision theory; past behavior of a node can be used to predict the future behavior of a node. This can be exploited by intelligent context aware adversaries to compromise a highly reputed node and then use it to abuse the system. Moreover, the development of several watchdog modules is based on the fact that majority of nodes in the neighborhood have not been compromised. In a nutshell, there are limits to which a homogeneous system can provide security; some form of hierarchy is needed. For instance, some high-end trusted nodes can be deployed to periodically check the status of nearby nodes. Similarly a secure data mule can be made to

periodically traverse through the network to perform this status check. This opens a lot of new issues – What should be the density of these high-end nodes? What should be the period of data mule?

Abuses: Reputation based systems have been found to be vulnerable to several abuses such as bad-mouthing, ballot stuffing attacks etc. [19]. We have incorporated special design features in our system, such as propagating only good reputation information, aging the reputation information, appropriately weighing the second hand information etc. to counter these attacks. We have taken a pessimistic approach of making the system as much secure as possible at the cost of efficiency. In general, more efficient operating points can be explored for RFSN.

5. Countermeasures for Malicious Environment

Attacks against the physical world manifest themselves at a network level. These attacks results in forming a vicious loop of learning and verification: How can a network verify whether what it is trying to learn is valid or not? The lack of complete global picture at a node restricts the applicability of any node-level solutions such as RFSN. As a first step towards developing countermeasures, we have carried out a broad classification of the existing physical world scenarios - non-cooperative (battlefield), neutral (environmental) and cooperative (monitoring with RFIDs tags). We envision developing different customized solutions for these three different types of scenarios.

The approach of modeling and prediction can be used for neutral physical processes where inconsistencies will arise due to inherent environmental noise and not due to malicious security breaches. Thus, if the network observes a huge discrepancy between the predicted and the sensed results; it can conclude that something is wrong. However a similar approach will not work for non-cooperative physical processes such as intrusion detection. An adversary can act in a completely random fashion. We propose to thwart these attacks by introducing redundancy on the sensing channel. Thereby, instead of relying on a single sensor modality such as temperature, the decision of intrusion must be taken through an efficient multimodal fusion of temperature, acoustic and camera sensing modalities. This can potentially thwart the attempt of a compromise by an adversary on a single sensor modality such as insertion of heat source affects temperature.

We note that we have just scratched the surface in this domain and these approaches still require a lot of thought and investigation.

6. Conclusions

In absence of adequate security, deployment of many applications of sensor networks could be curtailed. Only recently researchers have started looking into this matter and testimony to this is the development of many security protocols, judiciously designed to operate on the resource constrained sensor nodes. However, all the existing work has concentrated on providing secure communication using tools from cryptography. Cryptography presents an efficient mechanism for node authentication and maintaining data confidentiality and integrity.

We highlight some novel characteristics of these networks leading to unconventional attacks and system failures where cryptographic solutions are not sufficient. Cryptography cannot provide data authentication needed for countering misbehavior from internal adversaries, faulty nodes or abuses against the physical world. On the basis of these observations, we motivate the need of integrating tools from domains such as economics, statistics and data analysis with cryptography to facilitate the development of high integrity sensor networks.

One of the promising approaches that we are currently investigating, RFSN, is to develop a community of trustworthy sensor nodes at runtime based upon the behavior of these nodes. Sensor nodes maintain reputation for other nodes and use it to evaluate their trustworthiness. RFSN provides a scalable, diverse, unified and generalized approach for countering all types of misbehavior resulting from malicious and faulty nodes in the system. The lightweight modular architecture of RFSN has been designed keeping into mind the resource constraint nature of nodes, making it an apt solution for the development of trustworthy sensor networks.

References

[1] C. Karlof, D. Wagner, "Secure routing in sensor networks: Attacks and countermeasures", *Elsevier AdHoc Networks journal*, May 2003.

[2] J. P. Hubaux, L. Buttyan, S. Capkun, "The quest for Security in Mobile Ad hoc networks", ACM Mobihoc), October 2001.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, D. Tygar, "SPINS: Security Protocols for Sensor Networks", *Wireless Networks Journal*, September 2002.

[4] C. Karlof, N. Sastry, D. Wagner. TinySec: Link Layer Encryption for Tiny Devices. http://www.cs.berkeley.edu/~nks/tinysec/.

[5] J. Deng, R. Han and S. Mishra. The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks", *IPSN*, April, 2003.

[6] L. Eschenauer, V. D. Gligor, "A key Management Scheme for Distributed Sensor networks" *ACM CCS*, November 2002.

[7] H. Chan, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks" IEEE Symposium on Security and Privacy, 2003.

[8] D. Liu, P. Ning, "Establishing pairwise keys in distributed sensor networks" *ACM CCS*, October 2003.

[9] Withheld for anonymous review.

[10] A. Perrig, J. Stankovic, D. Wagner, "Security in Wireless Sensor Networks", *Communications of the ACM*, 2004.

[11] B. Przydatesk, D. Song, A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks", *ACM SenSys*, 2003.

[12] F. Ye, H. Luo, S. Lu, L. Zhang, "Statistical En-route Detection and Filtering of Injected False Data in Sensor Networks", *IEEE Infocom 2004*.

[13] R. L. Trivers. The evolution of reciprocal altruism. Quarterly review of biology. 46:35-57.

[14] P. Resnick, R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's Reputation System", *NBER workshop on empirical studies of electronic commerce*, 2000.

[15] S. Buchegger, J. L. Boudec, "Performance analysis of the CONFIDANT protocol", *ACM Mobihoc*, 2002.

[16] P. Michiardi, R. Molva, "CORE: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks", *Communication and Multimedia Security*, September, 2002.

[17] L. Xiong, L. Liu, "A reputation-based trust model for peer-to-peer ecommerce communities", *IEEE conference on e*-commerce, 2003.

[18] A. Jsang and R. Ismail, "The Beta Reputation System", *In Proceedings of the 15th Bled Electronic Commerce Conference*, June 2002.

[19] C. Dellarocas, "Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems", *ICIS*, 2000.