Handbook of Research on Developments and Trends in Wireless Sensor Networks:
From Principle to Practice

Hai Jin
Huazhong University of Science and Technology, China

Wenbin Jiang
Huazhong University of Science and Technology, China

Information Science
REFERENCE

INFORMATION SCIENCE REFERENCE
Hershey · New York

Director of Editorial Content:	Kristin Klinger
Director of Book Publications:	Julia Mosemann
Acquisitions Editor:	Mike Killian
Development Editor:	Beth Ardner
Publishing Assistant:	Kurt Smith
Typesetter:	Devvin Earnest
Quality control:	Jamie Snavely
Cover Design:	Lisa Tosheff
Printed at:	Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

Library of Congress Cataloging-in-Publication Data

Handbook of research on developments and trends in wireless sensor networks : from principle to practice / Hai Jin and Wenbin Jiang, editors.
p. cm.
Includes bibliographical references and index.
Summary: "This book showcases the work many devoted wireless sensor network researchers all over world, and exhibits the up-to-date developments of WSNs from various perspectives"--Provided by publisher.
ISBN 978-1-61520-701-5 (hardcover) -- ISBN 978-1-61520-702-2 (ebook) 1.
Wireless sensor networks--Research. I. Jin, Hai. II. Jiang, Wenbin.
TK7872.D48H357 2010
681'.2--dc22
2009052441

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

Chapter 13

Privacy and Trust Management Schemes of Wireless Sensor Networks: A Survey

Riaz Ahmed Shaikh
Kyung Hee University, Korea

Brian J. d'Auriol
Kyung Hee University, Korea

Heejo Lee
Korea University, Korea

Sungyoung Lee
Kyung Hee University, Korea

ABSTRACT

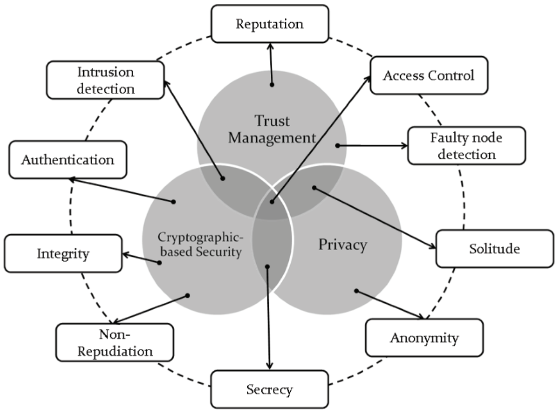
Until recently, researchers have focused on the cryptographic-based security issues more intensively than the privacy and trust issues. However, without the incorporation of trust and privacy features, cryptographic-based security mechanisms are not capable of singlehandedly providing robustness, reliability and completeness in a security solution. In this chapter, we present generic and flexible taxonomies of privacy and trust. We also give detailed critical analyses of the state-of-the-art research, in the field of privacy and trust that is currently not available in the literature. This chapter also highlights the challenging issues and problems.

INTRODUCTION

Security solutions based on cryptography are mainly used to provide protection against security threats, such as fabrication and modification of messages, unauthorized access, etc. For this purpose, assorted security mechanisms such as authentication, confidentiality, and message integrity are used. Additionally, these security mechanisms highly rely on a secure key exchange mechanism [Shaikh et al., 2006a]. However, these cryptography based security mechanisms alone are not capable of pro-

DOI: 10.4018/978-1-61520-701-5.ch013

Figure 1. Relationship between privacy, cryptographic-based security and trust



viding robustness, reliability and completeness in a security solution. They can only be achieved by incorporating privacy and trust features as described below.

Privacy features such as route anonymity of the data packets, identity anonymity of nodes and their locations are mainly used to provide protection against security threats such as traffic analysis and eavesdropping. Additionally, these privacy features could also be used to provide protection against security threats such as camouflage [Walters et al., 2006]. Therefore, the incorporation of these privacy features with cryptographic-based security mechanisms add to the degree of completeness of a security solution.

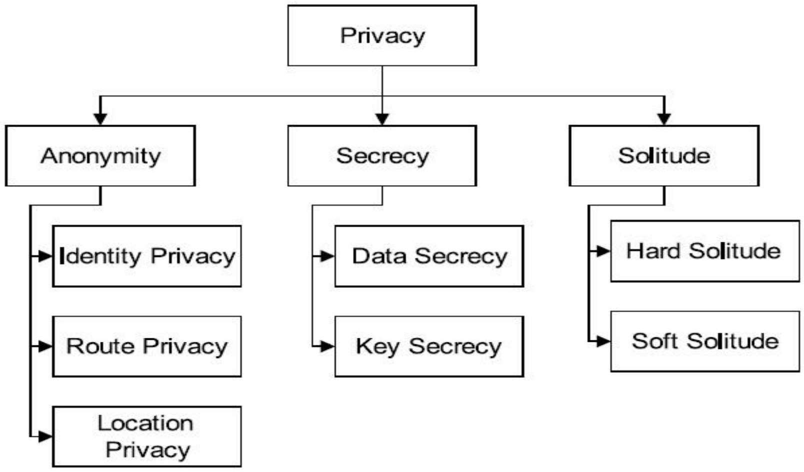
Trust management features, such as reputation is used to provide corresponding access control based on the judgment of the quality of sensor nodes and their services [Walters et al., 2006]. Also, it is used to provide complete reliable routing paths which are free from any malicious, selfish and faulty nodes [Liu et al., 2004]. Therefore, incorporation of trust management features with cryptographic-based security mechanisms help in increasing robustness and reliability of the overall security solution.

The soft relationship between privacy, trust, and cryptographic-based security is shown in Figure 1. This figure illustrates the related aspects of these terms with other commonly found terms used in the security domain. For example, secrecy is a mutual feature of cryptographic-based security and privacy aspects. In order to provide secrecy (also referred to as confidentiality), cipher algorithms (such as AES, DES) are used to prevent disclosure of information from any unauthorized entity. Similarly, an intrusion detection system may need a trust management feature such as reputation as well as a cryptographic-based security feature such as integrity checking to detect any malicious nodes. In like manner, solitude, which is used to isolate a node from the network either willingly or forcefully, is a mutual feature of trust and privacy aspects.

Current research so far seems to intensively focus on the cryptographic-based security aspects of wireless sensor networks. Many security solutions have been proposed such as SPINS [Perrig et al., 2002], TinySec [Karlof et al., 2004], LEAP [Zhu et al., 2003] and LSec [Shaikh et al., 2006b] etc., but surprisingly, less importance is given to privacy and trust issues of wireless sensor networks. Privacy and trust are as important as other security issues and they also contribute in increasing the degree of completeness and reliability of a security solution as discussed above.

In this chapter, we focus on the importance of privacy and trust establishment in wireless sensor networks. In Sections 2 and 3, we present generic and flexible taxonomies of privacy and

Figure 2. Taxonomy of privacy



trust respectively. These taxonomies are based on our specific experience with wireless sensor networks. Apart from these taxonomies, these sections also contain a detailed description of the privacy and trust issues of wireless sensor networks. This description is currently not available in the literature [Chan & Perrig, 2003; Djenouri et al., 2005; Perrig et al., 2004; Shaikh et al., 2006c; Walters et al., 2006]. Also, this chapter contains critical analyses of the state-of-the-art research work. Additionally, this chapter also highlights the challenging problems and issues in the field of privacy and trust in wireless sensor networks. Finally, last section concludes the chapter.

PRIVACY

Taxonomy

Privacy generally refers to "ability to control the dissemination of information about oneself" [Anderson, 2001]. In the wireless sensor network domain, so far privacy is mainly provided from anonymity [Misra & Xue, 2006; Ozturk et al., 2004; Wadaa et al., 2004;] and/or secrecy perspective [Karlof et al., 2004; Park & Shin, 2004; Perrig et al., 2002; Zhu et al., 2003]. However, neither anonymity nor secrecy is capable of providing complete privacy. In real life, we observe that complete privacy is gained through three independent but interrelated ways; *anonymity*: when an individual's true identity remains unidentified; *secrecy*: when an individual or a group's information remains protected from disclosure, and *solitude*: when one needs a temporal isolation in which an individual can not serve any request [DeCew & Judith, 2006]. Therefore, in order to achieve full privacy, we need to ensure that all these aspects: anonymity, secrecy, and solitude should be addressed. These three elements are further divided into sub categories as shown in Figure 2.

Anonymity provides three types of privacy protections, identity privacy, route privacy, and location privacy [Zhu et al., 2004].

- **Identity privacy:** No node can get any information about the source and destination nodes. Only the source and destination nodes can identify each other. Also, the source and destination nodes have no information about the real identities of the intermediate forwarding nodes.
- **Route privacy:** No node can predict the information about the complete path (from

source to destination) of the packet. Also, a mobile adversary can not get any clue to trace back the source node either from the contents and/or directional information of the captured packet(s).

- **Location Privacy:** No node can get to know any information about the location (either in terms of physical distance or number of hops) of the sender node except the source, its immediate neighbors and the destination.

Secrecy generally refers to the practice of hiding some information. Information is classified into two categories; one is the secrecy of actual sensed data (also referred as data confidentiality) forwarded by a sensor node to the specific destination and the other is key secrecy that is required to cipher data.

Solitude refers to the condition that a node goes into the state of isolation for a specific period of time. During that interval, the node cannot fulfill jobs nor can it provide services such as packet forwarding to the other nodes. We have categorized solitude into two types. *Soft solitude* refers to the node's decision to be in the solitude state. *Hard solitude* means that other node(s) in a compact or a command node decide to isolate a particular node.

Table 1 gives the classification of proposed privacy schemes (i.e. SAS & CAS [Misra and Xue, 2006], PFR PFR PFR [Ozturk et al., 2004], PSR PSR PSR [Kamat et al., 2005], SIGF SIGF SIGF [Wood et al., 2006], CEM CEM CEM [Ouyang et al., 2006], GROW GROW GROW [Xi et al., 2006], DIRL DIRL DIRL [Shaikh et al., 2008a]) of wireless sensor networks based on our proposed taxonomy. These schemes are discussed comprehensively in next section.

State-of-the-Art Research

Current research so far sees privacy either from a secrecy perspective or from an anonymity perspective. As mentioned earlier, full privacy consists of three elements: secrecy, anonymity, and solitude. Unfortunately, no solution, in the wireless sensor network domain, can guarantee the triumph of all these three elements in a single solution. In this section, we present the critical analysis of current state-of-the-art research work done so far in the field of privacy in wireless sensor networks.

Anonymity Schemes

In the wireless sensor network domain, some applications demand anonymity, for example, a panda-hunter application [Ozturk et al., 2004]; in which the *Save-The-Panda* organization has deployed sensor nodes to observe the vast habitat for pandas. Whenever any sensor node detects some panda it will make observations, e.g. activity, location, and periodically forward those to the sink node via some multi-path routing strategy.

Table 1. Application of privacy taxonomy

		SAS & CAS	PFR	PSR	SIGF	CEM	GROW	DIRL
Anonymity	Identity	Yes	No	No	No	No	No	Yes
	Route	Depending on routing scheme	Yes	Yes	Yes	Depending on routing scheme	Yes	Yes
	Location	No	Yes	Yes	Yes	Yes	Yes	Yes
Secrecy	Data	Yes	NA	NA	Yes	NA	NA	Yes
	Key	Yes	NA	NA	Yes	NA	NA	Yes
Solitude	Soft	No	No	No	No	No	No	No
	Hard	No	No	No	No	No	No	No

In this scenario, a hunter can try to capture the pandas by back-tracing the routing path until it reaches the source sensor nodes. Therefore, in order to prevent the hunter from back-tracing, the route and location anonymity mechanisms must be enforced. Similarly, in a battlefield application scenario, "the location of a soldier should not be exposed if he initiates a broadcast query" [Xi et al., 2006].

Traditionally, a number of various anonymity schemes have been proposed such as DC-Network [Chaum, 1988], Crowds [Reiter & Rubin, 1998], Onion Routing [Reed et al., 1998], Hordes [Shields & Levine, 2000], ARM [Seys & Preneel, 2006] etc. The most common approach used in these schemes is the employment of cover traffic. Cover traffic represents the dummy packets that are transmitted along with the original packets to the different destinations. In addition to cover traffic, some schemes use pseudonyms for assigning identities to the nodes. The objective of using cover traffic is to make an attacker clueless about the original packet and its destination. This kind of approach is not often suitable for traditional wired networks because it can cause a large amount of traffic overhead. Also these schemes have high computational cost mainly due to encryption and decryption of not only of the original packets but also of the dummy packets as well. These common problems make traditional anonymity schemes especially unsuitable for wireless sensor networks that operate in highly resource constraint environment.

PFR: Ozturk et. al. (2004) proposed a phantom routing scheme for wireless sensor networks that helps in preventing the location of a source node from the attacker. In this scheme, each message reaches the destination in two phases; 1) a walking phase in which the message is unicasted in random fashion within first h_{walk} hops and 2) a message flooding phase in which the message is flooded using the baseline flooding technique. In the first phase, the authors have introduced a bias in the random selection that makes it a directed walk from a pure random walk. The purpose of this approach is to minimize the chances of creating routing loops. However, this approach may incur delays. For example, because of a directed walk, the message may always move away from the base station. Thus, this approach is suitable for the applications that are not time sensitive. The main advantage of this scheme is that source location privacy protection improves as the network size and intensity increase because of the high path diversity. However, if the network size increases, the flooding phase consumes more energy, which in turn reduces the life time of the network.

PSR: Kamat et al. (2005) proposed a phantom single-path routing (PSR) scheme that works in a similar fashion as original phantom routing scheme [Ozturk et al., 2004]. They refer to the earlier one phantom-flood routing (PFR) scheme. The major difference between these two schemes is that, after the walking phase, the packet will be forwarded to the destination via a single path routing strategy such as shortest path routing mechanism. This scheme consumes less energy and requires marginally higher memory (each node need to maintain routing tables) as compared to the phantom-flood routing scheme. The major limitation of this scheme is that it only provides protection against a weaker adversary model.

SAS & CAS: Misra & Xue (2006) proposed two schemes for establishing anonymity in clustered wireless sensor networks. One is called Simple Anonymity Scheme (SAS) and other is called Cryptographic Anonymity Scheme (CAS). Both schemes are based on various assumptions such as sensor nodes are similar, immobile, consist of unique identities, and share pair-wise symmetric keys. The SAS scheme uses dynamic pseudonyms instead of a true identity during communications. Each sensor node needs to store a given range of pseudonyms that are non-contiguous. Therefore, the SAS scheme is memory inefficient. However, the CAS scheme uses keyed hash functions to generate pseudonyms. This makes it more memory efficient as compared to the SAS, but it requires more computation power.

SIGF: Wood et al. (2006) have proposed a configurable secure routing protocol family called Secure Implicit Geographic Forwarding (SIGF) for wireless sensor networks. The SIGF scheme is based on Implicit Geographic Forwarding (IGF) protocol [Blum et al., 2003], in which, a packet is forwarded to the node that lies within the region of a 60◦ sextant, centered on the direct line from the source to the destination. This approach reduces the path diversity and leads to only limited route anonymity is achieved. The SIGF protocol is mainly proposed by keeping security in mind. That is why some of the privacy aspects have not been covered such as identity privacy. Also, this protocol is unable to provide data secrecy in the presence of identity anonymity. Another drawback of this protocol is that, when there is no trusted node within a forwarding area, it will forward packet to the un-trusted node. So, the reliability of a path is affected.

GROW: Xi et al. (2006) proposed a Greedy Random Walk (GROW) scheme for preserving location of the source node. This scheme works in two phases. In the first phase, the sink node will set up a path through random walk with a node that acts as a receptor. Then the source node will forward the packet(s) towards the receptor in a random walk manner. Once the packet(s) reaches the receptor, it will forward the packet(s) to the sink node through the pre-established path. Here the receptor is acting as a central point between the sink and the source node for every communication session. The selection criteria of trustworthy receptors are not defined.

CEM: Ouyang et al. (2006) proposed a Cyclic Entrapment Method (CEM) to minimize the chance of an adversary to find out the location of the source node. In the CEM, when the message is sent by the source node to the base station, it activates the pre-defined loop(s) along the path. An activation node will generate a fake message and forward it towards the loop and original message is forwarded to the base station via specific routing protocol such as shortest path. Energy consumption in the CEM scheme is mainly dependent upon the number of loops in the path and their size.

DIRL: Shaikh et al. (2008a) have proposed a data privacy mechanism and two identity, route, and location privacy algorithms (IRL and r-IRL) for wireless sensor networks. We refer to this work as DIRL. The unique thing about the DIRL scheme is that it provides data secrecy in the presence of identity privacy. Also, the DIRL scheme assures that all packets will reach their destination by passing through only trusted intermediate nodes. From the memory and energy consumption point of view, the DIRL scheme is not very good in comparison with some other existing schemes such as PSR [Kamat et al., 2005]. However, at the modest cost of energy and memory, the DIRL scheme provides more privacy features (data, identity, route, and location) along with the attributes of trustworthiness and reliability.

Table 2 gives the summary of proposed privacy preserving schemes, i.e. PFR [Ozturk et al., 2004], PSR [Kamat et al., 2005], SAS & CAS [Misra & Xue, 2006], SIGF [Wood et al., 2006], CEM [Ouyang et al., 2006], GROW [Xi et al., 2006] and DIRL [Shaikh et al., 2008a].

Secrecy

Secrecy is generally used to hide the contents of the message from unauthorized access, but it is not used to hide the source and destination identity. Overall, secrecy is achieved through the combination of different security mechanisms such as authentication and confidentiality. Additionally, these security services highly rely on a secure key exchange mechanism [Shaikh et al., 2006a]. Quite recently, many security solutions have been proposed such as SPINS [Perrig et al., 2002], LEAP [Zhu et al., 2003], TinySec [Karlof et al., 2004], LiSP [Park and Shin, 2004], SBKH [Michell & Srinivasan, 2004], LSec [Shaikh et al., 2006b], MUQAMI [Raazi et al., 2007], etc. These provide various security services such

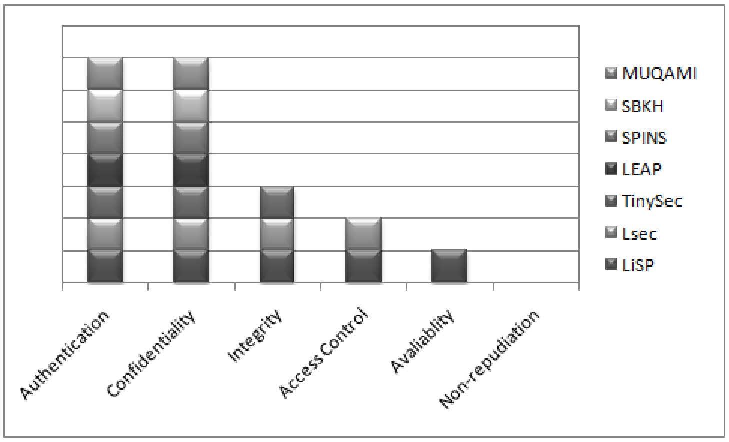
Table 2. Summary of privacy preserving schemes of WSNs

	PFR	PSR	SAS & CAS	SIGF	CEM	GROW	DIRL
Required information for routing	ID of destination	Routing table (e.g. dest. ID, # of hops etc.)	Depending on a routing scheme	Own, dest., & neighborhood locations	Depending on a routing scheme	Routing table (e.g. dest. D, receptor ID etc.)	Own, dest., & neighborhood locations
Transmission Mechanism	1st phase: Point-to-point; 2nd phase: Broadcast	Point-to-point	Depending on a routing scheme	Point-to-point	Point-to-point	Point-to-point	Point-to-point
Decision place for forwarding	1st phase: Transmitter; 2nd phase: Receiver	Transmitter	Depending on a routing scheme	Transmitter	Transmitter	Transmitter	Transmitter
Criteria for forwarding packet to next hop	1st phase: random; 2nd phase: flooding	1st phase: random; 2nd phase: shortest in terms of hops	Depending on a routing scheme	Randomly select any trusted node lies in forwarding region	Depending on a routing scheme	1st phase: random; 2nd phase: Predefined path	Randomly select any trusted node

as authentication, confidentiality, and message integrity. A high level qualitative comparison of these schemes is shown in Figure 3. This figure illustrates that the authentication, confidentiality, and integrity are well accommodated. However others (access control, availability, and non-repudiation) are not. A detailed description of each scheme is given below.

LEAP: Zhu et al. (2003) have proposed the security mechanisms: Localized Encryption and Authentication Protocol (LEAP), and a key management protocol for large scale distributed wireless sensor networks. In order to meet different security requirements, LEAP provides the support of four types of keys for each sensor node: 1) unique secret key that is shared between each sensor node and the base station, 2) pairwise key shared between each pair of neighboring nodes, 3) cluster key shared with multiple neighboring nodes, and 4) a group key that is shared by all the

Figure 3. Comparison of security protocols



nodes in the network. If a node has *d* neighbors, it needs to store one individual key, *d* pairwise keys, *d* cluster keys and one group key. The authors have employed the uTESLA (Perrig et al., 2002) protocol for broadcast authentication. However, in order to add more security such as inter-node authentication, the authors have used a hop-by-hop authentication strategy in which each node must authenticate the packet before forwarding it to the next hop. For this purpose, each node needs to store a one-way key chain of length *L* and most recent authenticated key of each neighbor. Therefore, each node needs to store total 3*d*+2+*L* keys.

SPINS [Description of this protocol has been taken from our published paper [Shaikh et al., 2006]**:** Perrig et al., (2002) have proposed a security protocols suite called SPINS for wireless sensor networks. SPINS consist of two building blocks, SNEP and uTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness where as uTESLA provides authenticated broadcast for severely resource constraint environments. For data confidentiality a symmetric encryption mechanism is used in which a secret key called the master key is shared between sensor nodes and the base station. SNEP uses a one-time encryption key that is generated from the unique master key. SNEP uses MAC function for two party authentications and checking data integrity. SPINS is based on a binary security model which means that either it provides maximum security or it does not provide any security. Usage of source routing scheme in SPINS makes the network vulnerable to traffic analysis [Undercoffer et al. 2002].

TinySec: Karlof et al. (2004) have proposed a secure architecture for wireless sensor networks called TinySec. TinySec is the first fully implemented link layer cryptography-based security protocol that provides authentication, integrity, and confidentiality by adding less than 10% of energy, latency, and bandwidth overhead [Shaikh et al., 2006c]. TinySec architecture comprises of two modes; 1) Authenticated encryption (TinySec-AE) mode, in which TinySec encrypts the payload (data) and authenticate the packet with a MAC. 2) Authentication only (TinySec-AH) mode, in which TinySec authenticates the entire packet with the MAC. TinySec protocol is tightly tied-in with Berkeley TinyOS. Therefore, it can not be used for general sensor network model [Perrig et al., 2004].

LiSP: Park and Shin (2004) have proposed the Lightweight Security Protocol (LiSP) that makes a tradeoff between security and resource consumption through efficient re-keying mechanism. This re-keying mechanism has a number of features such as: efficient key broadcasting, which does not require any retransmissions or acknowledgements; implicit authentication of new keys without incurring any additional overhead; seamless key refreshments; detection and recovery of lost keys. The LiSP protocol does not have any control packets or any type of retransmission that makes it energy efficient and secure against DoS attacks. LiSP provides the support of authentication, confidentiality, data integrity, access control and availability [Shaikh et al., 2006c]. In LiSP, each node need to save atleast eight keys therefore it is memory efficient. Also, the computation cost of LiSP is very low because on average it needs to compute less then three hash computations.

SBKH: Michell & Srinivasan, (2004) have proposed lightweight security protocol called State Based Key Hop (SBKH) for low power devices such as sensor nodes. SBKH achieves authentication, confidentiality, and integrity. In this protocol, two communicating nodes share common knowledge about RC-4 states. These states are used to generate cipher streams. These states remain the same for the pre-defined duration known only to two communicating nodes and will be reinitialized only when the base key changes. This approach gives the benefit of providing less computation overhead as compared to the traditional WEP and WPA 1.0 security solutions where RC-4 states are reinitialized for every packet.

However, the security strength of this scheme is mainly depended on a stronger key management and distribution scheme.

LSec: Shaikh et al., (2006b) have proposed the Lightweight Security (LSec) protocol for wireless sensor networks. LSec provides authentication, access control, confidentiality, and integrity of sensor nodes with simple key exchange mechanism. It works in three phases: 1) Authentication and authorization phase that is performed by using symmetric scheme, 2) Key distribution phase which involves sharing of random secret key by using asymmetric scheme and 3) Data transmission phases which involves transmission of data packets in an encrypted manner. LSec is memory efficient that requires 72 bytes to store keys. Also, it introduces 74.125 bytes of transmission and reception cost per connection.

MUQAMI: Raazi et al., (2007) have proposed a key management scheme for clustered sensor networks called MUQAMI. In MUQAMI, the responsibility of key management is divided among a small fraction of nodes within a cluster. Also, during the normal network operation, this responsibility can be transferred from one node to another with minimal overhead. This eradicates any single point of failure in the network. Also, this scheme is highly scalable and it eradicates all the inter-cluster communication. Lastly, it does not require all nodes to participate in key management, which reduces the security overhead substantially. This scheme is mainly designed for large-scale sensor networks. This scheme is more susceptible to collusion attacks [Moore, 2006] than other schemes such as LEAP+ [Zhu et al., 2006]. Its parameters should be chosen carefully in order to avoid collusion attacks.

Solitude

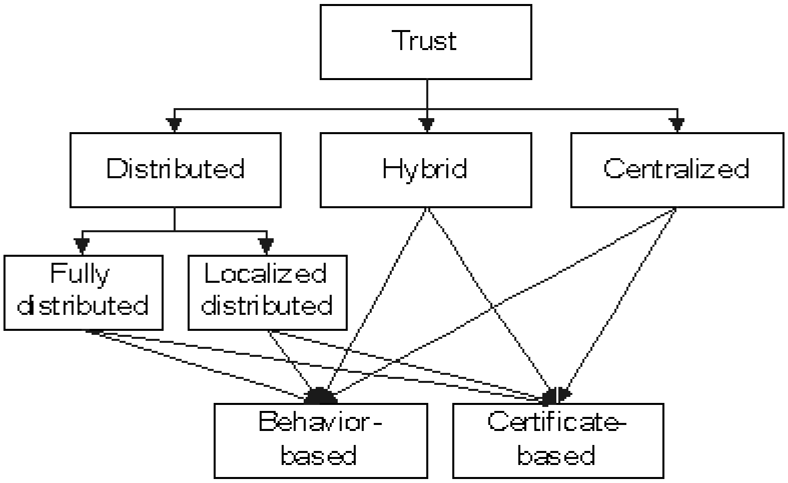
As we mentioned earlier, so far the concept of solitude is not used for achieving privacy in the wireless sensor networks. The concept of solitude could be applied in different ways. For example, soft solitude is achieved whenever any node does not want to participate in communication due to any reason such as to preserve energy etc, then that node will broadcast message to all its neighboring nodes. That message contains the node's state change information to solitude state for specific time. Once this message is received by the member nodes, they will no longer consider the solitude node for the purposes of forwarding a packet; virtually considers that the node is an un-trusted node. After the passage of some time, a node's state will reset to original (trusted or un-trusted) state. In order to provide protection against spoofing, receiving node will first perform an Angle of Arrival (AoA) and single strength check [Durresi et al., 2007], which will ensure that the packet was sent by the legitimate source node. Many other AoA-based localization techniques have been specifically proposed for sensor networks such as [Nasipuri & Li, 2002, Rong & Sichitiu, 2006]. Any one of them could be used. The pseudo-code of a Soft Solitude Algorithm (SSA) is given Algorithm 1.

Hard solitude could also be achieved with the help of trust values. If any node is considered to be un-trusted based on its trust value, that node will not be able to participate in a communication for a given period of time. For example, some intrusion detection techniques [Michiardi & Molva, 2002; Buchegger & Boudec, 2002] proposed for ad-hoc networks have the ability to gradually isolate the node(s) in case the node(s) are found to be

Algorithm 1. SSA

```
Receive Packet Pkt
Get NID = GetNodeID(Pkt)
if checkAoA(Pkt) = true then
    Set timer $\Delta t$;
    Set state = $NID_{state}$;
    while $\Delta t$ = true do
        $NID_{state}$ remain untrusted;
    end while
    $NID_{state}$ = state;
else
    Detect $spoof_{pkt}$;
end if
```

Figure 4. Taxonomy of trust



malicious or untrusted. However, those schemes require continuous monitoring and collection of information about intrusions at various places that increases overhead, and make them unsuitable for wireless sensor networks [Bhuse, 2007].

Challenging Issues

The main challenging issue that we are facing here is: "Having limited memory, computational capability and transmission/reception power of wireless sensor networks, is it practically possible to achieve full privacy?" It is not feasible to maintain complete privacy all the time in wireless sensor networks, not only due to the technological constraints but also due to the changing characteristics of application and the network itself. In general, privacy is a dynamic need at every level in wireless sensor networks. Applications, nodes and communication packets require different levels of privacy throughout their operation. Thus, privacy cannot be maintained at the same level all the time and an effective privacy scheme should efficiently cater for the dynamic privacy needs at all levels in wireless sensor networks. Hence, in this type of environment, the best way to achieve privacy is in a flexible and adaptive manner. Here flexible means that the scheme should support variable levels of privacy and adaptive means that with respect to time and demand, the solution should automatically adjust the required level of privacy. This kind of flexibility and adaptability is currently not available in the presently proposed privacy solutions of wireless sensor networks.

Another challenging problem is to protect various aspects of privacy (as mentioned earlier) against three different ways of privacy disclosure mechanisms [Walters et al., 2006]. One is by traffic analysis [Deng et al., 2004], second is by eavesdropping [Djenouri et al., 2005] and third is by camouflage [Walters et al., 2006]. Traffic analysis means that an attacker can get access to the information like "who is talking to whom?" based on that information, the attacker can infer the role and activities of each sensor node in the network. Eavesdropping means that an attacker can get the information like "what nodes are talking about?" and camouflaging means that an attacker can masquerade (via newly inserted nodes or via compromised nodes) as a normal node to attract the packets to pass through it.

TRUST MANAGEMENT

Taxonomy

Trust management schemes are classified into three categories: centralized, distributed and hybrid as shown in Figure 4.

Centralized trust management (CTM) schemes (e.g. [Blaze et al., 1999; Resnick et al., 2000]) consist of a single globally trusted server that determines the trust values of every node in the network. This gives the benefit of lesser computational overhead at the sensor node because most of the trust calculation is performed at centralized trusted server that has no constraints of computational power and memory. This approach however has the drawbacks of a single point of failure, which makes it least reliable. Also, it suppresses the underlying fact that different nodes may have different trust values about a particular given node [Theodorakopoulos & Baras, 2006]. For large scale sensor networks, centralized trust schemes are not suitable because the total routing cost for the exchange of trust values of a sensor node with the base station is quite energy expensive, especially when the base station is located far from the node. Therefore centralized approach introduces large communication overhead in the sensor network.

Distributed trust management (DTM) schemes (e.g. [Boukerche et al., 2007; Ganeriwal & Srivastava, 2004]) also do not work well for large-scale sensor networks. In the distributed approach, every node locally calculates the trust values of all other nodes in the network that increases the computational cost. Also each node needs to maintain an up-to-date record about the trust values of the entire network in the form of a table. The size of the table is directly proportional to the size of the network which results in a large memory consumption. Each sensor node maintains its own trust record and that gives the benefit of less communication overhead because a node does not need to contact with some centralized server. The distributed approach is more reliable than the centralized one because it has no single point of failure. In the wireless sensor network domain, some researchers use restricted DTM approach, in which sensor nodes only maintains the trust value about its neighboring nodes only e.g. [Ganeriwal & Srivastava, 2004]. We refer to that approach as a localized DTM approach and the earlier one as a fully DTM approach, e.g. [Boukerche et al., 2007]. The major drawback of the localized DTM approach is that it introduces delay and dependency whenever any node wants to evaluate trust of distant nodes. This is due to the fact that trust is established "dynamically at runtime using the chain of trust relationships between neighboring nodes" [Ganeriwal & Srivastava, 2004].

Hybrid trust management (HTM) schemes (e.g. [Krishna & Maarof, 2003; Shaikh et al., 2006a]) contain the properties of both centralized as well as distributed trust management approaches. The main objective of this approach is to reduce the cost associated with trust evaluation as compared to distributed approaches. This scheme is used with clustering schemes, in which cluster-head acts as a central server for the whole cluster. This approach is more reliable than the centralized one but less reliable than the distributed one. Each node needs to maintain the record of only member nodes, which gives the benefit of less memory consumption than the distributed approach. For intra-cluster communication, nodes need to contact the cluster head. It introduces more communication overhead in the network as compared to the distributed one.

The advantages and disadvantages of all three approaches are summarized in Table 3. All these three trust management approaches are further classified into two categories [Aivaloglou et al., 2007]: certificate-based trust management approach and behavior-based trust management approach. In the certificate-based trust management approach, trust is mainly based on the provision of a valid certificate assigned to a target node by a centralized certification authority or by other

Table 3. Advantages and disadvantages of trust management approaches

	Advantages	Disadvantages
Centralized	• Least computational overhead. • Least memory usage.	• Least reliable (single point of failure). • Most communication overhead.
Distributed	• Most Reliable (no single point of failure). • Scalable.	• Most computational overhead. • Most memory usage.
Hybrid	• Less communication overhead than centralized. • Less memory consumption than distributed. • Less computational overhead than distributed. • More reliable and scalable than centralized.	• Large computational overhead then centralized. • Large memory requirement than centralized. • Less scalable and reliable than distributed.

Table 4. Application of trust taxonomy

		Certificate-based	Behavior-based
Centralized		-	-
Hybrid		-	GTMS [Shaikh et al.,2009]
		[Aivaloglou et al., 2007]	
Distributed	Fully	ATRM [Boukerch et al., 2007]	-
	Localized	-	PLUS [Yao et al., 2006], RFSN [Ganeriwal & Srivastava, 2004], T-RGR [Liu et al., 2007]

trusted issuer. In the behavior-based trust management approach, an entity calculates the trust values by continuous direct or indirect monitoring of other nodes.

Table 4 gives the classification of proposed trust management schemes of wireless sensor networks based on our proposed trust taxonomy. These schemes are discussed in more comprehensive manner in next section.

State-of-the-Art Research

Research on trust management schemes for wireless sensor networks is in its infancy state. Few schemes have been proposed that are discussed below in chronological order. Our discussion in [Shaikh et al., in press] is extended with additional detail below.

RFSN: Ganeriwal et al. (2004, 2008) have proposed the Reputation based Framework for Sensor Network (RFSN) where each sensor node maintains the reputation for neighboring nodes. On the basis of that reputation trust values are calculated. The RFSN scheme follows the localized distributed approach and borrows some design features from several existing works in the literature. It uses Bayesian formulation for representing reputation of a node. The RFSN scheme assumes that the node would have enough interactions with the neighbors so that the reputation (beta distribution) can reach to a stationary state. If the mobility is at a higher rate, reputation information will not stabilize and it may degrade its performance. Therefore, this kind of architecture is most suitable for stationary networks as compared to the mobile networks. In the RFSN scheme, nodes are classified into two categories: cooperative and not cooperative. Trust formulation approach of RFSN scheme can not cope with uncertainty situations [Chen et al., 2007]. Also, in their scheme no node is allowed to disseminate bad reputation information. It is resilient against bad-mouthing [Sun et al., 2008] and ballot stuffing attacks [Ganeriwal and Srivastava, 2004] but at the cost of system efficiency, as nodes cannot share bad experiences with each other.

ATRM: Boukerch et al. (2005, 2007) have proposed the Agent based Trust and Reputation Management (ATRM) scheme for wireless sensor networks. The ATRM is based on a clustered wireless sensor networks and calculates trust in a fully distributed manner. Every sensor node holds a local mobile agent that is responsible for administrating trust and reputation of hosting node. ATRM assumes that there is a trusted authority which is responsible for generating and launching mobile agents. It also assumes that mobile agents are resilient against malicious nodes that try to steal or modify information carried by the agent. The major advantage of the ATRM scheme is that they use mobile agents for trust calculation which reduces the bandwidth consumption and time delay. The ATRM scheme work in two phases: 1) Network Initialization phase and 2) Service offering phase. In the first phase, the Agent Launcher (AL) distributes the mobile agents called Trust and Reputation Assessor (TRA) to each node. As long as node has local TRA, it is in service offering phase, in which it is ready to provide trust and reputation management services. This phase is composed of four sub-services: r-certificate acquisition, t-instrument issuance, r-certificate issuance, and trust management routine.

- The *r*-certificate acquisition is pre-transaction service whose objective is to find out the reputation value of the other node. This will be performed by the exchange of certificate request (CertReq) and reply (CertRep) messages. At the end of this service node will decide whether it should start transaction or not.
- The *t*-instrument issuance is a post transaction service whose objective is to evaluate trust value based on the recent context. This will be performed by the exchange of *t*-Instrument issuance (InstrIssument) and acknowledgement (ACK) messages.
- The *r*-Certificate Issuance service is executed periodically by replica TRAs based on the *t*-Instruments of their hosts. Since t- *t*-Instruments are context-specific, therefore in this process single reputation value is calculated based on all context's value.
- The trust management routine is also periodically carried out by every replica TRA to maintain the evaluation table on its hosting node. In each run, this routine will eliminate the any record from the table that is older then specific threshold time.

PLUS: Yao et al. (2006) have proposed Parameterized and Localized trUst management Scheme (PLUS) for sensor networks security. The authors adopt a localized distributed approach and trust is calculated based on either direct observations or indirect observations. Trust calculation mechanism involves the combination of six parameters: 1) ordering, 2) integrity checking, 3) confidentiality checking, 4) responsibility checking, 5) positivity checking and 5) cooperative checking. The involvement of so many parameters makes this scheme less generic and more complex. For example in 'ordering', node checks whether the packet forwarded by node *i* is really coming from the base station or not. For this purpose, they assume that all the important control packets generated by the base station must contain hashed sequence number (HSN). Based on that HSN it performs checking. If the check is passed then the trust value of the forwarding node will increase. The involvement of the HSN in control packets introduces two problems: 1) it increases the size of the packet that results in higher consumption of the transmission and reception power, 2) it increases the computational cost at the sensor node because sensor node needs to verify the control packet that contains the HSN. Also, in 'positivity' checking case, judge node monitors the suspected node *i* whether the node has participated in the exchange of opinions as well as whether it has sent report measurement to the base station with an appropriate frequency. This parameter forces the sensor nodes to remain in promiscuous mode all the time. In the PLUS scheme, node is classified into four categories: 1) Distrust (untrustworthy), 2) Minimal (low trust), 3) Average (common trustworthy), and 4) Good (trustworthy). However the mechanism of computing boundaries of four trust levels is missing.

T-RGR: Liu et al. (2007) have proposed a very simple trust management scheme for Resilient Geographic Routing (T-RGR) scheme. Their trust algorithm works in a localized distributed manner, in which each node monitors the behavior of the one-hop neighbors. If neighboring node successfully forwards the packet it will increase the trust value by a constant parameter, δt, and if it drops the packet then the source node will decrease its trust value by another constant parameter, Δt. If the trust value of a particular node is greater than the predefined threshold value, then the node will be considered as a trusted node, otherwise it will be un-trusted. In their paper, the authors do not mention the mechanism to calculate those three constant parameters that make their scheme non-adaptive. The main advantage of their scheme is that it is not only simple and easy to implement but it also consume less memory and energy. The main problem in their scheme is that each node only relies on its direct monitoring for the calculation of a trust value. This makes their scheme vulnerable to collaborative attacks.

FTSN: Aivaloglou et al. (2007) have proposed Flexible Trust establishment Framework for Sensor Networks (FTSN) but it is still in initial phases. The unique thing about the FTSN is that it combines the features of certificate-based and behavior-based trust establishment approaches. Some subset of nodes in the network performs certificate–based trust evaluation and some subset of nodes, called supervision nodes in the network; perform behavior-based trust evaluation. A certificate validation is performed locally and is distributed before the deployment of the sensor nodes in the field. These certificates are signed by offline trust management authorities. Since this scheme is based on pre-deployment knowledge, so it is suitable for static sensor network environment. Nodes are either classified into trusted or un-trusted. Support of un-certain evidence is not available in this framework.

GTMS: Shaikh et al. (2009) have proposed lightweight Group-based trust management scheme (GTMS) for clustered wireless sensor networks. The unique thing about the GTMS scheme is that in contrast to traditional trust management approaches, which always focus on trust values of individual users, the GTMS scheme evaluates the trust of a group of users. That group based approach gives the benefit of less memory consumption. GTMS calculates the trust value based on direct or indirect observations. Direct observations represent the number of successful and unsuccessful interactions and indirect observations represent the recommendations of trusted peers about a specific node. For example, a sender will consider an interaction as successful if the sender receives an assurance that the packet is successfully received by the neighbor node and that node has forwarded the packet towards the destination in an unaltered fashion.

The GTMS works with two topologies. One is the intra-group topology where distributed trust management is used. The other is inter-group topology where centralized trust management approach is employed. For the intra-group network, each sensor that is a member of the group, calculates individual trust values for all group members. Based on the trust values, a node assigns one of the three possible states: 1) trusted, 2) un-trusted or 3) un-certain to other member nodes. After that, each node forwards the trust state of all the group member nodes to the CH. Then, centralized trust management takes over. Based on the trust states of all group members, a CH detects the malicious node(s) and forwards a report to the base station. On request, each CH also sends trust values of other CHs to the base station. Once this information reaches the base station, it assigns one of the three possible states to the whole group. On request, the base station will forward the current state of a specific group to the CHs. This methodology helps to drastically reduce the cost associated with trust evaluation of distant nodes. [Shaikh et al.,2009]

GTMS is intrusion-tolerant and provides protection against malicious, selfish and faulty nodes. Authors have provided detailed theoretical and simulation-based analysis and evaluation from the perspective of security resiliency, communication overhead, memory overhead and energy consumption analysis. Results show that GTMS scheme is lightweight and more suitable for large-scale wireless sensor networks.

Table 5 gives a qualitative comparison of the proposed schemes based on number of different parameters as discussed below:

- **Trust-based on direct observations:** Represents the trust value that is calculated based on the personal interaction experience with other nodes and/or via monitoring of nodes which reside inside its radio range.
- **Trust-based on indirect observations:** Represents the value that is obtained from the recommendations of the peer nodes.
- **Trust levels:** Depending on the scope and functionality, various trust management schemes provide support for different trust levels. Minimally, we can classify the nodes into the two categories of trusted and un-trusted.
- Dependency on routing scheme: There are various routing schemes that have been proposed for wireless sensor networks. If a proposed trust management scheme is independent of any specific routing strategy then that scheme is considered to be a generic scheme.

Challenging Issues

The main research problem is "How to establish dynamic trust relationships in large scale wireless sensor networks?" This problem needs to be investigated within two network environments:

- **Static wireless sensor network environment:** In which both sensor nodes and the base station are stationary and each sensor node has a unique identity.
- **Mobile wireless sensor network environment:** In which sensor nodes and base station both are mobile. Sensor nodes may or may not have unique identities.

General research challenges that arise in the design of trust management schemes for both the network environments are:

- How to make our trust management scheme lightweight? Here lightweight means scheme should consume less energy, low memory and less computation power.
- How to make our trust management scheme resilient against security threats?

Table 5. Comparative features of trust management schemes

	RFSN	ATRM	PLUS	GTMS	T-RGR	FTSN
Trust-based on direct observations	Yes	Yes	Yes	Yes	Yes	Yes
Trust-based on indirect observations	Yes	No	Yes	Yes	No	Yes
Trust levels	2	-	4	3	2	2
Dependency on routing scheme	Any	Any clustered based RS	PLUS_R	Any clustered based RS	Any geographic RS	Any

If any node in the network has been compromised by an intruder and starts sending false information then the other nodes in the network should be able to detect that.

- How to make our trust management scheme flexible and robust?

By flexible we mean that the trust management scheme should be independent of any topology of sensor networks. By robust we mean that it should be reliable enough to provide accurate trust values in a timely manner. The specific issue that is related to the mobile wireless sensor network environment is, "How to maintain the trust level when a node is moving among different clusters of the network?"

In general, trust calculation at each node, in fact, measures the confidence in node reliability. Ideally network traffic conditions such as congestion, bandwidth, etc should not affect the trust attached to a node. Assume that node *A* sends data to node *B*, but because of packet loss due to congestion, packets do not reach node *B* successfully. In this case, node *A* will think that node *B* is not cooperating and not providing the required service. So node A will reduce the trust level of node *B*. This is a very challenging problem that how such intermittent failures which occur due to bad network parameters can be filtered automatically and the trust actually reflects the correct cooperative metric of node *B*. So far, not much focus has been given on this issue.

There are many application scenarios in which sensor nodes do not have unique identities or the identities should remain hidden for achieving anonymity in wireless sensor networks [Misra and Xue, 2006; Olariu et al., 2005]. So the challenging problem is: without knowing identities, how to establish and maintain trust between communicating nodes? In order to calculate trust, various schemes keep the track of past behavior of other nodes, here the issues are:

- Node should keep the record of how many past interactions?
- What weight should be given to old interactions and very recent interactions? and
- What weight should be assigned to the direct observations and to the indirect observations?

CONCLUSION

Current research so far focuses on the security issues of wireless sensor networks. Although many survey papers are available in the security domain of wireless sensor networks, but we did not find any work in the literature which discusses the privacy and trust issues of wireless sensor networks in detail. In this chapter, we have given critical analysis of the current state-of-the-art research work done so far in the field of privacy and trust of wireless sensor network domain. We also presented generic and flexible taxonomies of privacy and trust that are based on our own research experience with wireless sensor networks. At the end, we also highlighted the challenging issues and problems of privacy and trust that need to be resolved.

REFERENCES

Aivaloglou, E., Gritzalis, S., & Skianis, C. (2007). Towards a flexible trust establishment framework for sensor networks. *Telecommunication Systems*, *35*(3), 207–213. doi:10.1007/s11235-007-9049-x

Anderson, R. J. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis, IN: Publisher Wiley.

Bhuse, V. S. (2007). Lightweight intrusion detection: A second line of defense for unguarded wireless sensor networks. *PhD thesis, Dept. of Comp. Sci., Western Michigan University*.

Blaze, M., Feigenbaum, J., Ioannidis, J., & Keromytics. (1999). A. The keynote trust management system. In *RFC2704*.

Blum, B., He, T., Son, S., & Stankovic, J. (2003). *IGF: A state-free robust communication protocol for wireless sensor networks* (Tech. Rep. CS-2003-11). Dept. of Comp. Sci. University of Virginia, USA.

Boukerche, A., & Li, X. (2005). An agent-based trust and reputation management scheme for wireless sensor networks. *48th annual IEEE Global Telecommunications Conference* (pp. 1857–1861). St. Louis, MO: IEEE Press.

Boukerche, A., & Li, X., & EL-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, *30*(11-12), 2413–2427. doi:10.1016/j.comcom.2007.04.022

Buchegger, S., & Boudec, J. L. (2002). Performance analysis of the CONFIDANT protocol. In *Proceedings of the 13th ACM Symp. on Mobile Ad Hoc Networking and Computing* (pp. 226–236). Lausanne, Switzerland: ACM Press.

Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *Computer*, *36*(10), 103–105. doi:10.1109/MC.2003.1236475

Chaum, D. L. (1988). The dinning cryptographers problem: unconditional sender and recipient untraceability. *Journal of Cryptographyg*, *1*(1), 65–75.

Chen, H., Wu, H., Zhou, X., & Gao, C. (2007). Reputation-based trust in wireless sensor networks. *Int. Conference on Multimedia and Ubiquitous Engineering*, (pp. 603–607), Korea: IEEE Computer Society.

DeCew & Judith. (2006). Privacy. In Zalta, E. N., (ed.), *The Stanford Encyclopedia of Philosophy (Fall 2006 Edition)*, Stanford, CA: Metaphysics Research Lab, CSLI, Stanford University.

Deng, J., Han, R., & Mishra, S. (2004). Countermeasures against traffic analysis attacks in wireless sensor networks (Tech. Report CU-CS-987-04), Comp. Sci. Dept, University of Colorado, Boulder.

Djenouri, D., Khelladi, L., & Badache, A. (2005). A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications Surveys and Tutorials*, *7*(4), 2–28. doi:10.1109/COMST.2005.1593277

Durresi, A., Paruchuri, V., Durresi, M., & Barolli, L. (2007). Anonymous routing for mobile wireless ad hoc networks. *International Journal of Distributed Sensor Networks*, *3*(1), 105–117. doi:10.1080/15501320601069846

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transaction on Sensor Networks*, *4*(3), 1–37. doi:10.1145/1362542.1362546

Ganeriwal, S., & Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. *ACM Security for Ad-hoc and Sensor Networks*, (pp. 66–67). New York: ACM Press.

Kamat, P., Zhang, Y., Trappe, W., & Ozturk, C. (2005). Enhancing source-location privacy in sensor network routing. In *Proceedings of the 25th IEEE Int. conf. on Distributed Computing Systems*, (pp. 599–608), Columbus, OH: IEEE Computer Society.

Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: a link layer security architecture for wireless sensor networks. In Proceedings of the 2*nd Int. Conf. on Embedded networked sensor systems*, (pp. 162–175), Baltimore, MD:ACM Press.

Krishna, K., & bin Maarof, A. (2003). A hybrid trust management model for MAS based trading society. *The Int. Arab Journal of Information Technology*, *1*(1), 60–68.

Liu, K., Abu-Ghazaleh, N., & Kang, K.-D. (2007). Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, *67*(2), 215–228. doi:10.1016/j.jpdc.2006.08.001

Liu, Z., Joy, A. W., & Thompson, R. A. (2004). A dynamic trust model for mobile ad hoc networks. In *Proceedings of the 10th IEEE Int. Workshop on Future Trends of Distributed Computing Systems*, (pp. 80–85), Suzhou, China: IEEE Computer Society.

Michell, S., & Srinivasan, K. (2004). State based key hop protocol: a lightweight security protocol for wireless networks. In *Proceedings of the 1st ACM international Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, (pp. 112-118). Venezia, Italy: ACM Press.

Michiardi, P., & Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the 6th IFIP conf. on communications and multimedia security*, (pp. 107–121), Portoroz, Slovenia: Kluwer Academic Publishers.

Misra, S., & Xue, G. (2006). Efficient anonymity schemes for clustered wireless sensor networks. *International Journal of Sensor Networks*, *1*(1/2), 50–63. doi:10.1504/IJSNET.2006.010834

Moore, T. (2006). A Collusion Attack on Pairwise Key Predistribution Schemes for Distributed Sensor Networks. In *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, pp. 251-255. IEEE Computer Society.

Nasipuri, A., & Li, K. (2002). A directionality based location discovery scheme for wireless sensor networks. In Proceedings of the *1st ACM international Workshop on Wireless Sensor Networks and Applications*, (pp. 105-111). Atlanta, Georgia, USA: ACM Press.

Olariu, S., Xu, Q., Eltoweissy, M., Wadaa, A., & Zomaya, A. Y. (2005). Protecting the communication structure in sensor networks. *International Journal of Distributed Sensor Networks*, *1*(2), 187–203. doi:10.1080/15501320590966440

Ouyang, Y., Le, Z., Chen, G., Ford, J., & Makedon, F. (2006). Entrapping adversaries for source protection in sensor networks. *2006 Int. Sym. on a World of Wireless, Mobile and Multimedia Network*, (pp. 23–34), Buffalo, NY: IEEE Computer Society.

Ozturk, C., Zhang, Y., & Trappe, W. (2004). Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks*, (pp. 88–93), Washington, DC: ACM Press.

Park, T., & Shin, K. G. (2004). LiSP: A lightweight security protocol for wireless sensor networks. *ACM Transaction on Embedded Computing Sys.*, *3*(3), 634–660. doi:10.1145/1015047.1015056

Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, *47*(6), 53–57. doi:10.1145/990680.990707

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: security protocols for sensor networks. *Wireless Networks*, *8*(5), 521–534. doi:10.1023/A:1016598314198

Raazi, S., Khan, A., Khan, F., Lee, S., & Song, Y.-J. (2007). MUQAMI: A locally distributed key management scheme for clustered sensor networks. In Etalle, S. and Marsh, S., (eds), *Int. Federation for Infor. Proc.*, (pp. 333–348). Boston: Springer.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, *6*(4), 482–494. doi:10.1109/49.668972

Reiter, M. K., & Rubin, A. D. (1998). Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, *1*(1), 66–92. doi:10.1145/290163.290168

Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (2000). Reputation systems: Facilitating trust in internet interactions. *Communications of the ACM*, *43*(12), 45–48. doi:10.1145/355112.355122

Rong, P., & Sichitiu, M. L. (2006). Angle of Arrival Localization for Wireless Sensor Networks. In *Proceedings of the 3rd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON '06)*, (pp. 374-382), Reston, VA: IEEE Communications Society.

Seys, S., & Preneel, B. (2006). ARM: Anonymous routing protocol for mobile ad hoc networks. In *Proceedings of the 20th Int. conf. on Advanced Information Networking and Applications*, (pp. 33–37), Vienna Austria: IEEE Press.

Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, S., Song, Y.-J., & Lee, H. (2008a). Network level privacy for wireless sensor networks. In *Proceedings of the 4th International Conference on Information Assurance and Security (IAS 2008)*, (pp. 261–266), Naples, Italy: IEEE Computer Society.

Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, S., Song, Y.-J., & Lee, H. (2009). Group-based Trust Management Scheme for Clustered Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, *20*(11), 1698–1712. doi:10.1109/TPDS.2008.258

Shaikh, R. A., Jameel, H., Lee, S., Rajput, S., & Song, Y. J. (2006a). Trust management problem in distributed wireless sensor networks. In *Proceedings of the 12th IEEE Int. Conf. on Embedded Real Time Computing Systems and its Applications*, (pp. 411–414). Sydney, Australia: IEEE Computer Society.

Shaikh, R. A., Lee, S., Khan, M. A. U., & Song, Y. J. (2006b). LSec: Lightweight security protocol for distributed wireless sensor network. In *11th IFIP Int. Conf. on Personal Wireless Comm., LNCS 4217*, (pp. 367–377), Albacete, Spain: Springer-Verlag.

Shaikh, R. A., Lee, S., Song, Y. J., & Zhung, Y. (2006c). Securing distributed wireless sensor networks: Issues and guidelines. In *Proceedings of the IEEE Int. Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing- vol. 2 - Workshops*, pp. 226–231, Taiwan: IEEE Computer Society.

Shields, C., & Levine, B. N. (2000). A protocol for anonymous communication over the internet. In *Proceedings of the 27th ACM conf. on Computer and communications security*, (pp. 33–42), Athens, Greece: ACM Press.

Sun, Y. L., Zhu, H., & Liu, K. J. R. (2008). Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine*, *46*(2), 112–119. doi:10.1109/MCOM.2008.4473092

Theodorakopoulos, G., & Baras, J. S. (2006). On trust models and trust evaluation metrics for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 318–328. doi:10.1109/JSAC.2005.861390

Undercoffer, J., Avancha, S., Joshi, A., & Pinkston, J. (2002). Security for Sensor Networks. Paper presented at *2002 CADIP Research Symposium,* Baltimore, MD.

Wadaa, A., Olariu, S., Wilson, L., Eltoweissy, M., & Jones, K. (2004). On providing anonymity in wireless sensor networks. In *Proceedings of the 10th Int. conf. on Parallel and Distributed Systems*, (pp. 411–418), California, USA: IEEE Computer Society.

Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2006). Wireless sensor network security: A survey. In Xiao, Y., (ed.), *Security in Distributed, Grid, and Pervasive Computing*, (pp. 367–410). CRC Press.

Wood, A. D., Fang, L., Stankovic, J. A., & He, T. (2006). SIGF: a family of configurable, secure routing protocols for wireless sensor networks. In *Proceedings of the 4th ACM workshop on Security of ad hoc and sensor networks*, (pp. 35–48). Alexandria, VA: ACM Press.

Xi, Y., Schwiebert, L., & Shi, W. (2006). Preserving source location privacy in monitoring-based wireless sensor networks. In *Proceedings of the Parallel and Distributed Processing Symposium (IPDPS 2006)*, Rhodes Island, Greece: IEEE Computer Society.

Yao, Z., Kim, D., & Doh, Y. (2006). PLUS: Parameterized and localized trust management scheme for sensor networks security. In *Proceedings of the 3rd IEEE Int. Conf. on Mobile Adhoc and Sensor Systems*, (pp. 437–446), Vancouver, Canada: IEEE Computer Society.

Zhu, B., Wan, Z., Kankanhalli, M. S., Bao, F., & Deng, R. H. (2004). Anonymous secure routing in mobile ad-hoc networks. In *Proceedings of the 29th IEEE Int. conf. on Local Computer Networks*, (pp. 102–108), Tampa, USA: IEEE Computer Society.

Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. In *Proceedings of the 10th ACM Conf. on Computer and Comm. security*, (pp. 62–72). NY: ACM Press.

Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sensor Networks*, *2*(4), 500–528. doi:10.1145/1218556.1218559

KEY TERMS AND DEFINITIONS

Centralized Trust Management: A single globally trusted server determines the trust values of every node in the network.

Distributed Trust Management: Every node locally calculates the trust values of all other nodes in the neighborhood or network.

Hard Solitude: Means that other nodes in a compact or a command node decide to isolate a particular node.

Identity Privacy: No node can get any information about the source and destination nodes. Only the source and destination nodes can identify each other. Also, the source and destination nodes have no information about the real identities of the intermediate forwarding nodes.

Location Privacy: No node can get to know any information about the location (either in terms of physical distance or number of hops) of the sender node except the source, its immediate neighbors and the destination.

Route Privacy: No node can predict the information about the complete path (from source to destination) of the packet. Also, a mobile adversary can not get any clue to trace back the source node either from the contents and/or directional information of the captured packet(s).

Soft Solitude: Refers to the node's decision to be in the solitude state.

Solitude: Refers to the condition that a node goes into the state of isolation for a specific period of time. During that interval, the node cannot fulfill jobs nor can it provide services such as packet forwarding to the other nodes.

Trust: Represents the level of confidence on other entity.