Towards an Optimized Reputation System for Security Aware Energy Efficient Geographic Routing in Wireless Sensor Networks

BY

ISMAT KHALED MAAROUF

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES
KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE
In
COMPUTER NETWORKS

June 2007
Contents

Acknowledgement .............................................................................................................. ii
List of Tables ...................................................................................................................... ix
List of Figures ..................................................................................................................... x
THESIS ABSTRACT ........................................................................................................ xiii
THESIS ABSTRACT (ARABIC) ......................................................................................... xiv

Chapter 1: Introduction ..................................................................................................... 1
  1.1 Motivation ................................................................................................................. 2
  1.2 Secure Routing Problem ......................................................................................... 6
  1.3 Secure Routing Goals ............................................................................................ 7
  1.4 Trust Aware Routing .............................................................................................. 8
    1.4.1 Definition ........................................................................................................ 8
    1.4.2 Importance ..................................................................................................... 9
  1.5 Problem Statement and Research Objectives ....................................................... 10
  1.6 Contributions ......................................................................................................... 12
  1.7 Thesis Organization ............................................................................................... 13

Chapter 2: Background and Literature Survey ................................................................. 14
  2.2 WSN Node Structure .............................................................................................. 16
  2.3 Routing Protocols in WSN .................................................................................. 18
  2.4 WSN vs. MANET .................................................................................................. 20
  2.5 Routing Attacks .................................................................................................... 22
Chapter 3: Reputation System Overview

3.1 Reputation System Framework

3.2 Customized Reputation System Overview

3.3 System Assumptions

3.4 Performance Evaluation Objectives
Chapter 4: Monitoring Component: Efficient Monitoring Procedure in Reputation Systems (EMPIRE)

4.1 EMPIRE Description ........................................................................................................ 41
   4.1.1 Procedure Description............................................................................................. 41
   4.1.2 Non Forwarding Attack Detection........................................................................ 43
   4.1.3 Why Probabilistic Approach.............................................................................. 44
   4.1.4 Assumptions.......................................................................................................... 45

4.2 Performance Measures and Simulation Setup.................................................................. 46
   4.2.1 Simulation Objectives............................................................................................ 46
   4.2.2 Performance Measures......................................................................................... 47
   4.2.3 Simulation setup.................................................................................................... 49
   4.2.4 Simulation Results and Analysis......................................................................... 50

4.3 Related Work.................................................................................................................. 56

4.4 Chapter Summary.......................................................................................................... 57

Chapter 5: Rating Component: Cautious Rating for Trust Enabled Routing (CRATER)

5.1 Cautious Assumptions.................................................................................................... 59

5.2 Rating Factors in CRATER .......................................................................................... 60
   5.2.1 Rating on First Hand Information FHI ............................................................... 61
   5.2.2 Rating on Second Hand Information SHI ......................................................... 66
   5.2.3 Rating on Neutral Behavior .............................................................................. 68

5.3 CRATER Evaluation........................................................................................................ 68

5.4 Related Work.................................................................................................................. 68

5.5 Chapter Summary.......................................................................................................... 70
Chapter 6: Reputation Systems-Independent Scale for Trust on Routing

(RESISTOR) .....................................................................................................................71

6.1 The Resistance Concept ......................................................................................... 72
6.2 RESISTOR Description ......................................................................................... 73
6.3 RESISTOR and CRATER Evaluation...................................................................... 75
6.4 How to Analyze RESISTOR Curve ........................................................................ 75
6.5 CRATER Evaluation Using RESISTOR ............................................................... 76
   6.5.1 Simulation Objectives ..................................................................................... 77
   6.5.2 Simulation Setup ............................................................................................. 77
   6.5.3 Results Analysis .............................................................................................. 78
6.6 Related Work.......................................................................................................... 84
6.7 Chapter Summary.................................................................................................. 85

Chapter 7: Response Component: Geographic, Energy and Trust Aware Routing

(GETAR) ...........................................................................................................................86

7.1 The Original Protocol: GEAR............................................................................... 88
   7.1.1 GEAR Description .......................................................................................... 88
7.2 The New Protocol: GETAR................................................................................... 91
   7.2.1 Basic Idea........................................................................................................ 91
   7.2.2 Forwarding in GETAR.................................................................................... 92
   7.2.3 The Risk Function r(.) ..................................................................................... 93
   7.2.4 Dissemination and Voids in GETAR.............................................................. 93
7.3 Simulation Objectives and settings ....................................................................... 94
   7.3.1 Objectives........................................................................................................ 94
Chapter 7: Simulation-based Evaluation

7.3.2 Assumptions ........................................................................................................ 95
7.3.3 Simulation Setup ............................................................................................... 95
7.3.4 Performance Measures .................................................................................. 96
7.3.5 Simulation Results and Analysis .................................................................... 98

7.4 Related work ....................................................................................................... 103
7.4.1 SAR .............................................................................................................. 103
7.4.2 TRANS ......................................................................................................... 104
7.4.3 RGR ............................................................................................................ 106
7.4.4 New Contributions as Compared to Previous Work .................................... 106

7.5 Chapter Summary ............................................................................................. 107

Chapter 8: Sensor Node Attached Reputation Evaluator (SNARE): Integrating
Reputation System Components ............................................................................... 108

8.1 Integration Approach ....................................................................................... 108
8.2 Network Model ............................................................................................... 110
8.3 Simulation Objectives ..................................................................................... 111
8.4 Simulation Results and Analysis .................................................................... 112
8.4.1 Varying NMA ............................................................................................ 112
8.4.2 Varying $T_{\text{update}}$ .................................................................................. 118
8.4.3 Varying $f_{\text{max}}$ ......................................................................................... 122
8.4.4 The Effect of Attacker Population in the Network ....................................... 123
8.4.5 Quick Analysis of Packet End-to-End Delay .............................................. 125

8.5 Conclusion ......................................................................................................... 127

Chapter 9: Adaptation Techniques for System Performance Optimization .......... 129
9.1 Adaptation Factors........................................................................................................ 130
  9.1.1 Attacker’s Location............................................................................................... 130
  9.1.2 Attack’s Time..................................................................................................... 130

9.2 Adaptation Techniques............................................................................................. 131
  9.2.1 Adapting $\beta$.................................................................................................. 131
  9.2.2 Adapting NMA.................................................................................................. 132

9.3 Simulation Objectives............................................................................................... 132

9.4 Simulation Results and Analysis............................................................................. 133
  9.4.1 Adaptation to attacker’s location...................................................................... 133
  9.4.2 Adaptation to Attacks’ Times......................................................................... 138

9.5 Conclusion.................................................................................................................. 143

Chapter 10: Conclusion and Future Work................................................................. 144
  10.1 Research Summary............................................................................................... 144
  10.2 Main Research Conclusions and Findings......................................................... 145
  10.3 Future Work and Further Research Directions................................................ 146

Glossary.......................................................................................................................... 150

Bibliography.................................................................................................................. 153

Vitae............................................................................................................................... 158
THESIS ABSTRACT

Name: Ismat Khaled Maarouf
Title: Towards an Optimized Reputation System for Security Aware Energy Efficient Geographic Routing in Wireless Sensor Networks

Major Field: COMPUTER NETWORKS
Date of Degree: June, 2007

Secure routing in wireless sensor networks is a crucial problem that has drawn the attention of researchers. One main type of security problems considering routing operation is misbehavior related attacks. In such attacks, the behavior of the malicious node is the distinguishing factor and not its identity. The motivation for tackling this problem comes directly from the highly constrained nature of WSN and its easy exposure to such attacks. The conventional approach in solving security problems is to adopt a crypto-based solution. Although such solutions are robust and cannot be replaced in some of their aspects, they do not provide a perfect and global coverage in the case of behavior related security. In this thesis work, another promising approach is adopted based on reputation systems. Reputation system based solution monitors routers activities and rates them accordingly which helps in making appropriate selection of routers in the future. Reputation based solutions have not been studied in depth as an appropriate solution for secure routing in wireless sensor networks due to wireless sensor networks constraints. The work in this thesis proposes a new reputation system approach that is more suited for WSN as a design target. The design focuses on security and resource usage efficiency. This research directs the attention towards system performance optimization. Under these lights, the work provides several new techniques to help in system optimization such as efficient monitoring, energy and trust aware routing and adaptation to security conditions.

MASTER OF SCIENCE DEGREE

King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia.

June, 2007
خلاصة الرسالة

الاسم: عصمت خالد معروف

عنوان الرسالة: نحو نظام صيغة أمثل لتسير جغرافي فعال ومدرك أمنيا في شبكات المجسسات اللاسلكية

الخصائص: شبكات الحاسب الآلي

تاريخ التخرج: حزيران "يونيو" 2007

يعتبر التسيرة الأمني في شبكات المجسسات اللاسلكية مشكلة معقدة تجنب اهتمام الباحثين. إحدى أنواع مشاكل التسيرة الأمني هو الهجمات المرتبطة بإساءة سلوك النطاق المعاداة. في مثل هذه الحالات سلوك النطاق المعاداة هو العامل المميز والأهم هو أننا لا يمكن استبدالها في بعض الجوانب إلا أنها لا توفر تغطية أمنية شاملة في الحالات المرتبطة بالسلوك. في هذه الرسالة نقوم بعرض طريقة أخرى للحل باستخدام نظام الصيغة. نظر الصيغة تعود على مراقبة نشطة المسيرات و من ثم تقييمها بالشكل المناسب للمسيرات في المستقبل. نظم الصيغة لتم دراستها مسبقاً بعث كحل مناسب لمشكلة التسيرة الأمني في مجال شبكات المجسسات اللاسلكية بسبب تعقيد هذه الشبكات. في هذه الرسالة نقدم طرحا جديداً لنظام صيغة أكثر تلاولاً مع شبكات المجسسات اللاسلكية كهدف للتصميم. يركز التصميم على الفعالية الأمنية وفعالية استخدام موارد الشبكة. ووجه البحث الاهتمام نحو مقارنة أداء النظام لأفضل مستوى. و في هذا الاعتبار يقدم العمل عدة تقنيات جديدة لمقارنة النظام لأداء الأمثل كتقنية المراقبة الفعالة و التسيرة المدرك بالطاقة والمدرك للثقة و التكيف حسب الظروف الأمنية.

درجة الماجستير في العلوم

جامعة الملك فهد للبترول والمعادن

حزيران "يونيو" 2007
Chapter 1

Introduction

The issue of secure routing in wireless and mobile computing is a major challenging design factor in different networking aspects. However, the problem gets more complicated when considering infrastructure-less networks that exhibit even more constraints and new types of attacks. Wireless sensor networks (WSN), which is an ad-hoc type of networks, is a clear representative case.

In the continuously and rapidly evolving area of wireless communication, the field of wireless sensor networks (WSN) comes into the picture as a very hot area of research in all its aspects. WSN is a multi-hop network that is actually one type of ad hoc networks. However, WSN draws the special attention of researchers due to the fact that it exhibits more constraints and critical conditions than normal ad hoc networks in terms of power sources, computing capabilities, memory capacity and other factors. This requires different approaches and protocol engineering directions from those applied to normal ad hoc networks.

One special aspect in WSN is the provision of secure routing. As mentioned previously, the nature of WSN complicates the security requirements and adds difficulties in solving security problems. In fact, secure routing in WSN is actually still not captured
well in the research field. One main reason is that the design of a routing protocol is biased towards solving the problem of power limitations and reducing communication overhead, while keeping security concerns in a later phase to be integrated with the current routing solutions.

One specific class of security problems in routing aspects in WSN is the exposure to attacks that are related to nodes’ activities and behavior in the network. Such attacks cannot be recognized by verifying nodes’ identities because most of these attacks are launched by compromised nodes or insider attacks; i.e. nodes belong to the same network community. Among different approaches in solving this problem, reputation system based solution is one technique that has generated enough interest among WSN research community. Reputation systems attempt to provide security by allowing different nodes to rate each other based on their routing activities and behavior analysis. When a node has an experience profile about its neighbors, it may select the node that it trusts more, and, hence, achieve a secure routing operation.

The work in this thesis investigates and proposes a reputation system solution for behavioral based attacks at the network layer as a provision of secure routing in WSN.

1.1 Motivation

In this work, we provide a reputation system based solution for routing security in WSN. We believe that such a solution approach is a feasible and applicable solution for the following reasons:

- Conventional security solution such as cryptography can successfully defend against outsiders’ attack. The mechanics of such solutions fail when the attack is
done by insiders or compromised nodes. Some of such attacks are intentionally performed like the misbehavior of selfish nodes and compromised nodes. Other attacks can be carried-out unintentionally by faulty nodes [1]. Thus, security systems like reputation based security solutions that have a mechanism to treat such attacks by behavior analysis are more suitable. This is especially true in networks where such misbehavior is very possible or even it is the dominant type of attacks, which is the case in WSN.

- In contrast to different secure routing mechanisms, reputation based systems provide a means for an adaptive and dynamic decision making and reaction at the individual node level behavior. Such features are needed in networks that exhibit dynamicity in nodes’ behavior like that in WSN.

- Most WSN deployments and applications invite a very dynamic networking nature. The current conditions and statistics of the network will change from time to time. The security system, thus, must accept to tune itself to these changes at the network level.

- WSN life and operation depends on the cooperation of nodes like any other ad hoc network. This implies that the security interest of a node is not only about itself but also about the whole network. As a result, such networks will prefer to communicate security information in order to keep the network healthy. This is an important feature of reputation systems. Node rating is one type of information that contributes to node’s decision making and can be communicated as second hand information. However, the node reaction is also important and affects other nodes’ decisions. Thus, the security system should have the feature of a consulted
and well-analyzed decision-making and behavior, which are core concepts in reputation systems.

- An interesting and important feature of any reputation system is that it follows a generalized and modular solution approach to fight against any attack in a general framework. The system then is customized to face a subset of these attacks. Thus, new attacks will be tackled by modifications in the details of the module of interest that does not require a complete system revision. For example, a new attack might require adjusting the monitoring and detection phase without touching other parts of the system. WSN are deployed in very hostile conditions that expect new attempts and attacks. Thus, it is better to support reputation systems in that regard rather than other solutions that can be totally and entirely useless with the occurrence of new misbehavior strategies.

In literature, there are different, but few, proposed reputation based solutions for secure routing in ad hoc networks. Very familiar examples include CONFIDANT (Cooperation Of Nodes – Fairness In Dynamic Ad-hoc Networks) [2], SORI (Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks) [3] and CORE (Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks)[4]. There are also other solutions that are close to the reputation systems but they do not follow the general mechanism. Examples are watchdog and pathrater as well as context-aware detection [5, 6].

As these solutions are applied to ad hoc networks, the conclusion of applying them to wireless sensor network as a type of ad hoc networks is not totally accurate. There are several reasons that show the need to have a special reputation system design and implementation that targets WSN. This differentiation comes from the following facts:
• Resource Constraints: An obvious difference between MANET and WSN is resource constraints. Resources include power, memory and processing capabilities. Although both networks suffer from resources deficiency, WSN are more constrained and limited by such resources, especially in power. Any protocol design and implementation targeting WSN from the physical to the application layer must consider resource usage optimization not as an additional feature in the system but as a main design goal. Therefore, an optimized approach must be considered when designing a reputation system for WSN.

• Conditions and Applications: Security conditions in WSN are different from general MANET networking type. As a result, the reputation based security system will be looking at providing solutions that satisfy these conditions that indeed implies different approaches for WSN and MANET as they differ in that aspect. Moreover, the risky environment that comes from the application types in WSN raises a remark of having security models that are different than MANET. What implies is a different view of reputation system for WSN.

• Underlying Routing Protocol: In contrast to MANET, DSR (Dynamic Source Routing) as a routing protocol is not the accurate or suitable choice for WSN for several reasons related to resource constraints and efficiency. Moreover, other routing protocols like GPSR (Greedy Perimeter Stateless Routing) [7] and GEAR (Geographic Energy Aware Routing protocol) [8] prove their outperformance compared to DSR. Thus, the implemented reputation systems in WSN should consider the operation of routing protocols that are more applicable than DSR.