SECURE-SPIN WITH HASHING TO SUPPORT MOBILITY AND SECURITY IN WIRELESS SENSOR NETWORK

MOHAMMAD HOSSEIN AMRI

UNIVERSITI TEKNOLOGI MALAYSIA

SECURE-SPIN WITH HASHING TO SUPPORT MOBILITY AND SECURITY IN WIRELESS SENSOR NETWORK

MOHAMMAD HOSSEIN AMRI

A project report submitted in partial fulfillment of the
Requirements for the award of the degree of
Master Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2013

This dissertation is dedicated to my family and my friend for their and her endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisors **Dr. Shukor Abd Razak** and **Dr. Anazida Zainal** for their constant support during my study at UTM. They inspired me greatly to work in this project. Their willingness to motivate me contributed tremendously to our project. I have learned a lot from them and I am fortunate to have them as my mentors and supervisors

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

Routing protocols with supporting mobility is a new area that these years attract many researchers; different protocols made to support different applications and needs. The existing routing protocols with support mobility often designed with no security in mind; so later other researchers tried to add security function to these protocols. Adding new and extra functionality (even security) sometimes brings other vulnerability. The Secure-SPIN is a routing protocol with support mobility that branched from SPIN protocol; the Spin protocol has no security, but Secure-SPIN tries to add security to it. During this extra functionality, the Secure-SPIN keeps its vulnerability to eavesdropping as SPIN does. This thesis tries to secure Secure-SPIN with utilizing hash function (SHA1), and with separating encryption and hash function from each other try to add new security feature. With dividing hash and encryption less or same level of energy will be use. In this thesis, mathematical prove used To prove security of proposed protocol. The proposed solution use extra energy but the energy consumption is low enough to ignore the extra energy usage in trade-off with more security.

ABSTRAK

Protokol penghalaan yang menyokong mobiliti adalah satu bidang baru yang mana dapat menarik ramai penyelidik; protokol yang berbeza dibuat untuk menyokong aplikasi yang berbeza dan keperluan. Protokol penghalaan sedia ada yang menyokong mobiliti sering direka tanpa memikirkan keselamatan; oleh itu, penyelidik yang lain telah mencuba untuk menambah fungsi keselamatan ke dalam protokol ini. Penambahan baru dan fungsi tambahan (walaupun keselamatan) kadang-kadang membawa kepada kelemahan lain. *Secure-SPIN* adalah protokol penghalaan yang menyokong mobiliti yang dicabangkan daripada protokol SPIN. Protokol SPIN tidak mempunyai faktor keselamatan, tetapi *Secure-SPIN* cuba untuk menambah faktor keselamatan ke dalamnya. Semasa penambahan fungi ini, *Secure-SPIN* masih mempunyai kelemahan untuk mencuri dengar sama seperti SPIN. Tesis ini cuba untuk selamatkan *Secure-SPIN* dengan menggunakan fungsi hash (SHA1), dan dengan memisahkan penyulitan dan fungsi hash daripada satu sama lain untuk cuba menambah ciri-ciri keselamatan yang baru. Tenaga yang kurang atau sama aras telah digunakan untuk pembahagian hash dan penyulitan . Dalam tesis ini, pembuktian matematik digunakan untuk membuktikan keselamatan protokol yang telah dicadangkan. Penyelesaian yang dicadangan menggunakan tenaga yang lebih tetapi penggunaan tenaga tersebut cukup rendah untuk diabaikan berbanding penggunaan tenaga bagi mendapatkan keselamatan yang lebih.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

Acronym	Description
WSN	Wireless Sensor Network
SPIN	Sensor Protocol for Information via Negotiation
AC	Authentication Code
PSAC	Private Session Authentication Code
REQ	Request Message
ADV	Advertisement Message
DATA	Data Message

CHAPTER 1

INTRODUCTION

1.1 Background of study

New development in “micro-electro-mechanical” ran to new low power and integrated digital electronic that helped us to make “disposable unattended sensors”. This development has fueled new research in possible applications in past years about addressing the possibilities of association among processing and sensing ambient and managing the sensing activity and data flow that nodes send to sink (BS)(Akkaya & Younis, 2005). This researches described basic capabilities of “wireless sensor network” and needed features that make network layer of WSN more robust and secure (Al-Karaki & Kamal, 2004).

Storage capacities, processing capabilities and energy of sensor nodes are narrow. Thus, they need careful “resource management” so make it compulsory to have “energy-awareness” in all protocol layer of a protocol stack. The problems associated to some layers (e.g. Physical and link layer) are common between applications and some researches focused only on “system level power awareness” capabilities like “dynamic voltage scaling”, “radio communication hardware”, “low duty cycle issues”, “system positioning” and “energy-aware MAC Protocols”. Network layer protocols’ goal is to find means for best energy-efficient routing protocol that will be reliable for communicating and expand life time of the network(Al-Karaki & Kamal, 2004).

Network layer is highly vulnerable to attacks and need to face with many security issues. There are many studies that consider security of routing protocols in WSN. Since the main purpose of those routing protocols was not security, improvements and studies to add security to them does not fulfill its job totally well. Attacks like selective forwarding, sinkhole attack, wormhole attack, Sybil attack, HELLO flood attack, ACK spoofing still make problems into sensor network(Karlof & Wagner, 2003). Unsolved security problems are making a vast study area about security issues.

Additional network that is similar to "sensor network" is "ad-hoc network" but sensor network in contrast to "ad-hoc networks" has a more communication outline. While the ad-hoc network usually supports routing between any pair of nodes. In WSN because of numerous features that differentiate Routing in "wireless ad hoc network" and "modern wireless communication" than "wireless sensor networks", routing becomes more confusing. Some special communications like many-to-one or many-to-many connection is not feasible to use as a routing protocol in WSN. For example, "many to one" connection and redundancy flow that nodes make does not let us make "global addressing scheme". Also in WSN routing protocols need to manage and exploit redundant flows to take care of scarce resources and basic constrains of Wireless Sensor nodes like "transmission power", "on-board energy", "processing capacity" and storage.

Traffic in "sensor networks" can be categorized to one of the following categories:

i. "One-to-many": A node (usually the sink (BS)) broadcasts a query or multicast control information to some sensor nodes.
ii. "Many-to-one": nodes send data to aggregation node or base station
iii. Local communication: communication between close nodes to synchronize or discover each other. It happens when a node broadcasts or unicast some query or data that only local nodes receive it.

It assumed that ad-hoc nodes have more constrain, but sensor nodes are still more limited than ad-hoc nodes. The most pressing of all of the resource constraints is energy limit. Nodes should be unattended after deployment and should be designed to work for a long time without battery replacement or recharging due to inaccessibility to nodes. It makes impossible or infeasible to replace or change nodes (Karlof & Wagner, 2003). When the mobility added to WSN, in resources, sensor nodes are more limited than ad-hoc network or MANETs, e.g. Battery limits the power in the sensor nodes, limited memory and limited processing capability of the sensor nodes, limited bandwidth etc. (Abolhasan, Wysocki, & Dutkiewicz, 2004).

Topologies of mobile sensor network in contrast to MANET networks and ad-hoc network, due to frequent death of the sensor nodes are highly dynamic; Link failure always may happen (even while data is transmitting) because death of nodes due to no battery supply or busy node or collision or other events. This necessitates retransmission of data, and it causes more energy. Mobility of the sink and sensor nodes may cause link failure of various point-to-point links. Also, sensor node mobility produces “station fading” (a Physical Layer phenomenon). Data transmission and movement affect the performance of the network in terms of “Bit Error Rate” and “Frame Error Rate”. Heavy traffic over some nodes may cause quick reduction of energy in those nodes, which may initiate death of those nodes in the future and may cause network barrier. Another cause of early death of some nodes is unbalanced load in the sensor nodes.(Deva Sarma *et al*., 2011)

The differences in the characteristic of ad-hoc network prevent routing solution of other networks to be useful in wireless sensor network. Routing protocols with support of mobility does not have a good security protection in the network layer, and secure routing protocols support no mobility, or if they do, they support mobility limited.

The secure routing in mobile wireless sensor network has overlooked. Unprepared nature of mobile network makes it hard to distinguish between untrusted and trusted nodes. Also, the dynamic nature of mobile networks makes it compulsory

for routing protocol to adapt itself to changes that happen so fast on the fly (Venkatraman & Agrawal, 2003). Moreover to design a good and robust secure routing protocol for “mobile wireless sensor network”, need to have security in mind, but the current available protocols do not consider security in network layer(Sarma, Kumar, & Kar, 2011).

The challenge is to get a satisfactory balance between security and performance, but constrains like energy, ram and process capability make valid methods in other networks an imperfect solution in wireless sensor network. Mobility of sensor nodes make confront of attacks harder than stable nodes to confront an attack; hence it is difficult to track down a node in a wide area. Also because of limits in energy it should be possible to add a new node to networks before the network die. To make it easy to deploy wide sensor network, new nodes need pre-configuration. These pre-configuration limit choices over cryptographic encryption. Constrain in one hand and pre-configuration in the other hand put a limit on possible encryption systems and sensor node characteristic; also it is possible for a node to be silent or be unattended for a period of the time, the node inattention increase the possibility of compromised key(Hu & Sharma, 2005).

Current protocols that support mobility are so limited and almost none of them designed with security in mind. SPIN is one of those protocols that support mobility, but it suffers from lack of security. There are some enhancements over SPIN protocol like Secure-SPIN and S-SPIN that both of them could not fulfill security goal perfectly. Problems in Secure SPIN make an empty area in the study about secure routing in mobile wireless sensor network.

1.2 Statement of the problem

The SPIN protocol designed with no security in mind. There is some improvement over SPIN, like Secure SPIN (Xiao & Wei, 2006), S-SPIN (Tang & Li, 2009) and MSWSN (Puthal, 2012), which all of them tried to add security to SPIN.

S-SPIN main Problem is focusing just on modeling, and the proposed model is vulnerable against Sybil attack. In S-SPIN, the encryption and the packet security method is unknown. The author tried to show how to prove security of a model without simulation. So security of proposed model is so basic that it cannot be reliable as a secure model.

In Secure-SPIN, there is vulnerability in authentication method. In the initial phase, the sink generate an "authentication code (AC)" and broadcast it, then the sensor to authenticate itself, take the AC and XOR it with its own key which generate "personal authenticate code (PSAC)" and send it back to sink. This method is vulnerable against eavesdropping because the AC and PSAC both send through the air and an adversary easily can listen to them and decrypt it to get sensor key.

MSWSN look like as promising routing protocol but since it derived from Secure-SPIN vulnerabilities carried into the protocol. The difference is that the PASC can be decrypt from ADV packet and impact of the vulnerability become so much higher than Secure-SPIN. In Secure-SPIN adversary only can find sensor key, but if the adversary listen to ADV packets, it also can decrypt key of Sink and nodes that are share between all nodes of network (Puthal, 2012).

1.3 Purpose of study

Wireless sensor network usage is growing in many part of modern life. The application that has different usage in Military or applications that have an impact on daily life like weather control systems is growing every day. Sensor nodes are a new concept that will affect daily life and for sure security is one crucial part of it (Huang, Bai, & Chen, 2007). Network layer security can strengths the reliability of sensor network since many attacks happen in the network layer. In sensor nodes, data transmission happen through air so the intruder can eavesdrop or act as a malicious router. This will stop packets delivery to destination and decrease reliability of the network. There are many researches to give security to available routing protocols. Also, the existing routing protocols with support mobility often designed with no security in mind; so later other researchers tried to add security function to these protocols. Extra and new functionality (even security) sometimes bring other vulnerability. The Secure-SPIN is a routing protocol with support mobility that branched from SPIN protocol; the Spin protocol has no security, but Secure-SPIN tries to add security to it. During this extra functionality, the Secure-SPIN keeps its vulnerability to eavesdropping as SPIN does. The purpose of this study is to solve vulnerabilities of secure-SPIN to have more security than existing one.

1.4 Objective of the study

The objectives of this study are:

i. To evaluate the current vulnerabilities of existing Secure-SPIN protocol.
ii. To propose improved Secure-SPIN protocol using the hash function
iii. To evaluate the proposed protocol in terms of security and energy efficiency.

1.5 Research question

- How to secure Secure-SPIN against eavesdropping?
- How to secure Secure-SPIN against forged AC?
- How to have security in all messages of Secure-SPIN?

1.6 Scope of the study

This study will focus on secure routing in mobile wireless sensor network to propose an enhancement for Secure-SPIN.

i. Secure-SPIN (original) and Improved Secure-SPIN will be check and validate.
ii. Security will consider mathematically.

1.7 Significance of the study

This study by study and evaluate existing solutions and focus on one or more characteristic of routing needs make it easier for further development in secure routing in mobile wireless sensor network.

Also, this study will aggregate the common ability of various security function in wireless sensor network, and clear different vulnerabilities in Secure-SPIN to help easier understanding to design middle-ware and routing protocol that add two heterogeneous network to each other. Moreover this study can be applied to other routing protocols.

1.8 Organization of Reports

Rest of this thesis organized as follow:

Chapter 2 provides a review of related works, conclude reasons about SPIN and describe how it fulfills requirements in mobile sensor network. At end secure protocols and especially secure method proposed for SPIN reviewed.

Chapter 3 provides the frame-work and methodology to improve the Secure-SPIN.

Chapter 4 provides the design of proposed improved protocol. During design, the theme of Secure-SPIN for better understanding preserved.

Chapter 5 provides the improved protocol with hash function compared with Secure-SPIN. The differences and benefit. Also, the attack scenario explained and described how the new proposed method mitigates those vulnerabilities. At the end, the impact of the proposed method on energy consumption discussed.

Chapter 6 provides discussion about limitations and future work and the effectiveness of the newly proposed model.

REFERENCES

Abolhasan, M., Wysocki, T. & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. *Ad hoc networks*, *2*(1), 1–22. Elsevier.

Albath, J. & Madria, S. (2007). Practical algorithm for data security (PADS) in wireless sensor networks. *Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access*, 9–16.

Albath, J. & Madria, S. (2009). Secure hierarchical data aggregation in wireless sensor networks. *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, 1–6.

Ashraf, A., Hashmani, M., Chowdhry, B. S., Mussadiq, M., Gee, Q. & Rajput, A. Q. K. (2008). Design and analysis of the security assessment framework for achieving discrete security values in wireless sensor networks. *Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on*, 000855–000860.

Hexmoor, H., Bhattaram, S. & Wilson, S. (2004). Trust-Based Security Protocols.

Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L. S. & Rubenstein, D. (2002). Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet. *ACM Sigplan Notices*, *37*(10), 96–107.

Kazatzopoulos, L., Delakouridis, C., Marias, G. & Georgiadis, P. (2006). ihide: Hiding sources of information in wsns. *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on*, 8–pp.

Marinescu, D. C., Yu, C. & Marinescu, G. M. (2008). A secure self-organizing sensor network. *Self-Adaptive and Self-Organizing Systems Workshops, 2008. SASOW 2008. Second IEEE International Conference on*, 114–119.

Quan, Z. & Jiuhao, L. (2009). Secure routing protocol cluster-gene-based for wireless sensor networks. *Information Science and Engineering (ICISE), 2009 1st International Conference on*, 4098–4102.

Stent, S. (2009). A Security Framework for Wireless Sensor Networks. *Communication and Networking*, 444–454. Springer.

Tubaishat, M., Yin, J., Panja, B. & Madria, S. (2004). A secure hierarchical model for sensor network. *ACM SIGMOD Record*, *33*(1), 7–13. ACM.

Wang, C., Sohraby, K., Li, B., Daneshmand, M. & Hu, Y. (2006). A survey of transport protocols for wireless sensor networks. *Network, IEEE*, *20*(3), 34–40. IEEE.

Wen, S., Du, R. & Zhang, H. (2006). A Segment Transmission Secure Routing Protocol for Wireless Sensor Networks. *Computational Intelligence and Security, 2006 International Conference on*, *2*, 1579–1582.

Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, *3*(3), 325-349. Retrieved from http://www.sciencedirect.com/science/article/pii/S1570870503000738

Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: a survey. *Wireless Communications, IEEE*. doi:10.1109/MWC.2004.1368893

Awwad, S. A. B., Ng, C. K., Noordin, N. K., & Rasid, M. F. A. (2011). Cluster Based Routing Protocol for Mobile Nodes in Wireless Sensor Network. *Wireless Personal Communications*, *61*(2), 251-281. Retrieved from http://dx.doi.org/10.1007/s11277-010-0022-8

Camilo, T. and Silva, J.S. and Boavida, F. (2006). Assessing the use of ad-hoc routing protocols in Mobile Wireless Sensor Networks. *Proc. CSMU*.

Cao, Z., Hu, J., Chen, Z., Xu, M., & Zhou, X. (2008). FBSR: feedback-based secure routing protocol for wireless sensor networks. *International Journal of Pervasive Computing and Communications*, *4*(1), 61-76. doi:10.1108/17427370810873110

Deva Sarma, H. K., Kar, A., & Mall, R. (2011). Energy efficient routing protocol for Wireless Sensor Networks with Node and Sink mobility. *2011 IEEE Sensors Applications Symposium*, 239-243. Ieee. doi:10.1109/SAS.2011.5739777

Hosseini Seno, S. A., Budiarto, R., & Wan, T.-C. (2011). A routing layer-based hierarchical service advertisement and discovery for MANETs. *Ad Hoc*

Networks, *9*(3), 355-367. Retrieved from http://www.sciencedirect.com/science/article/pii/S157087051000082X

Hu, F., & Sharma, N. K. (2005). Security considerations in ad hoc sensor networks. *Ad Hoc Networks*, *3*(1), 69-89. doi:10.1016/j.adhoc.2003.09.009

Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: a link layer security architecture for wireless sensor networks. *Proceedings of the 2nd international conference on Embedded networked sensor systems* (pp. 162-175). New York, NY, USA: ACM. doi:10.1145/1031495.1031515

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, *1*(2–3), 293-315.

Kumar, H., & Sarma, D. (2009). Energy Efficient Communication Protocol for a Mobile Wireless Sensor Network System, *9*(2), 386-394.

Li, X., & Nayak, A. (2010). Sink mobility in wireless sensor networks. *Sensor and Actuator Networks*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/9780470570517.ch6/summary

Luo, H., Ye, F., Cheng, J., Lu, S., & Zhang, L. (2005). TTDD: Two-Tier Data Dissemination in Large-Scale Wireless Sensor Networks. *Wireless Networks*, *11*(1-2), 161-175. Springer. doi:10.1007/s11276-004-4753-x

Nasser, N, Al-Yatama, A., & Saleh, K. (2012). Zone-based routing protocol with mobility consideration for wireless sensor networks. *Telecommunication Systems*. Department of Information Science, College for Women, Kuwait University, P.O. Box: 5969, Safat, 13060, Kuwait. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84857732792&partnerID=40&md5=c3284c210b091153c49f0f7d9522338b

Nasser, Nidal, & Chen, Y. (2007). SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks. *Computer Communications*, *30*(11–12), 2401-2412. Retrieved from http://www.sciencedirect.com/science/article/pii/S0140366407001727

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: security protocols for sensor networks. *Wirel. Netw.*, *8*(5), 521-534. Hingham, MA, USA: Kluwer Academic Publishers. doi:10.1023/A:1016598314198

Puthal, D. (2012). Secure data collection and critical data transmission technique in mobile sink wireless sensor networks.

Routing Protocols for Ad Hoc Mobile Wireless Networks. (2004). Retrieved from http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing.pdf

Sarma, D., Kumar, A., & Kar, B. (2011). Secure Routing Protocol for Mobile Wireless Sensor Network. *Symposium (SAS), 2011*. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5739778

Tang, L., & Li, Q. (2009). S-SPIN: A Provably Secure Routing Protocol for Wireless Sensor Networks. *2009 International Conference on Communication Software and Networks*, 620-624. Ieee. doi:10.1109/ICCSN.2009.8

Venkatraman, L., & Agrawal, D. P. (2003). Strategies for enhancing routing security in protocols for mobile ad hoc networks. *Journal of Parallel and Distributed Computing*, *63*(2), 214-227. doi:10.1016/S0743-7315(02)00065-5

Wood, A. D., Fang, L., Stankovic, J. A., & He, T. (2006). SIGF: a family of configurable, secure routing protocols for wireless sensor networks. *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks* (pp. 35-48). New York, NY, USA: ACM. doi:10.1145/1180345.1180351

Xiao, D., & Wei, M. (2006). Secure-spin: Secure sensor protocol for information via negotiation for wireless sensor networks. *Industrial Electronics and*, (c), 1-4. Ieee. doi:10.1109/ICIEA.2006.257149

Abolhasan, M., Wysocki, T. & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. *Ad hoc networks*, *2*(1), 1–22. Elsevier.

Huang, Q., Bai, Y. & Chen, L. (2007). An efficient route maintenance scheme for wireless sensor network with mobile sink. *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, 155–159.

Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L. S. & Rubenstein, D. (2002). Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet. *ACM Sigplan Notices*, *37*(10), 96–107.

Potlapally, N. R., Ravi, S., Raghunathan, A. & Jha, N. K. (2003). Analyzing the energy consumption of security protocols. *Proceedings of the 2003 international symposium on Low power electronics and design*, 30–35.

Wander, A. S., Gura, N., Eberle, H., Gupta, V. & Shantz, S. C. (2005). Energy analysis of public-key cryptography for wireless sensor networks. *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, 324–328.

Wang, C., Sohraby, K., Li, B., Daneshmand, M. & Hu, Y. (2006). A survey of transport protocols for wireless sensor networks. *Network, IEEE*, *20*(3), 34–40. IEEE.