SECURE ON-DEMAND ROUTING PROTOCOL IN WIRELESS SENSOR NETWORKS BASED ON ROUTE WEIGHT AND KNOWLEDGE SHARING

ALI FARROKHTALA

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

To my beloved family for their endless support and encouragement
and in the memory of my grandmother

ACKNOWLEDGEMENT

My First thanks are to the Almighty God. I then would like to express my deep-felt gratitude to my supervisor, Dr. Mohammad Abdur Razzaque, for his advice, encouragement, enduring patience and constant support. He was always providing clear explanations when I was lost and always giving me his time, in spite of anything else that was going on. Without his invaluable assistance, it would not have been possible for me to complete this thesis, and I am grateful for his guidance and attention in correcting this work.

Thanks to my family for their encouragement, support and love transmitted to me, my dear parents and beloved sister Shahla for always being there for me and their unwavering love that had shaped my mind and opened the doors of opportunity leading me to become the person I am today.

Thanks to all my friends, especially to Abouzar Azarpira, Armaghan Behnia, Babak Emami, Hesam Hasani Afshar, Pooria mobara, Saman Asadi and Sara Andalib for their time, understanding, wise advice and unconditional support and love that helped me during my master study.

ABSTRACT

Due to the rapid growth of wireless sensor network's applications, the lack of appropriate secure protocol is so sensible. Meanwhile, a huge number of researches have been done to fulfill these security principles but still there is not any approved standard in this field. Black hole attack as one of the most common insider attacks of Ad hoc networks has been targeted in this research. Black hole attack is occurred when one node or a group of compromised nodes begin to make a disruption in network routing through dropping of every received packet. Many security mechanisms are presented to detect and mitigate this attack that one of them is route weight method. However, our contribution is combining this technique with the knowledge sharing concept. In order to achieve this goal some modifications are applied to algorithm and source code of Ah hoc On-demand Distance Vector routing protocol. AODV is one of the lightweight protocols in the wireless network that is not secure by itself. As a result of employed mentioned security mechanisms into AODV make it possible to protocol continue to its procedure at the present of adversarial nodes and black hole attacks as far as a safe route exists between source and destination. Conversely, simulation results show that it caused a small amount of overload packet but still has great performance even in comparison to be other proposed protocols.

ABSTRAK

Oleh kerana pertumbuhan pesat aplikasi rangkaian sensor tanpa wayar, kekurangan protokol selamat yang sesuai begitu waras. Sementara itu, sejumlah besar penyelidikan telah dilakukan untuk memenuhi prinsip-prinsip keselamatan, tetapi masih tidak ada apa-apa piawaian yang diluluskan dalam bidang ini. Serangan lubang hitam sebagai salah satu daripada serangan dalaman yang paling biasa rangkaian ad hoc telah disasarkan dalam kajian ini. Serangan lubang hitam berlaku apabila satu nod atau sekumpulan nod dikompromi mula membuat gangguan dalam laluan rangkaian melalui menjatuhkan setiap paket yang diterima. Banyak mekanisme keselamatan dibentangkan untuk mengesan dan mengurangkan serangan ini salah seorang daripada mereka adalah kaedah berat laluan. Walau bagaimanapun, sumbangan kami adalah menggabungkan teknik ini dengan konsep perkongsian pengetahuan. Dalam usaha untuk mencapai matlamat ini beberapa pengubahsuaian digunakan untuk algoritma dan kod sumber Ah hoc On-permintaan Jarak Vector protokol routing. AODV adalah salah satu protokol ringan dalam rangkaian wayarles yang tidak menjamin dengan sendirinya. Hasil daripada bekerja mekanisme keselamatan yang dinyatakan dalam AODV membuat ia mungkin untuk terus protokol prosedur pada masa ini nod pertentangan dan serangan lubang hitam sejauh laluan yang selamat wujud di antara sumber dan destinasi. Sebaliknya, keputusan simulasi menunjukkan bahawa ia disebabkan jumlah yang kecil paket sarat tetapi masih mempunyai prestasi yang baik walaupun dalam perbandingan menjadi lain protokol dicadangkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Mobile ad-hoc networks are more complex than traditional wireless networks or Wireless local area networks. Since Wireless sensor networks are considered as a subcategory of ad-hoc network, it inherits almost every feature of ad-hoc networks such as no infrastructure existing, self-organization without any central fixed component. Nature of ad-hoc network makes them proper solution for disaster area communications or hard establishment situations. Recent wireless technology advances provide the opportunities of sufficient resources to implement dynamic communications networks. However, it also came with several security issues and makes it vulnerable to serial attacks and challenging to security aspects [1].Wireless sensors are little wireless devices with an ad-hoc communications system over wireless channels, creating Wireless Sensor Networks (WSNs) which attract much attention to this area throughout the last decade. In addition, it purveyed a variety of useful application scenarios such as medical, military, transportation, robotic, environment monitoring and automation. Healthy operations of WSNs can be the very interested area for adversaries to make disruptions to these vital application's areas. For instance, it is very significant to deliver accurate data to the sink in critical proper time. Therefore, attack resilient should be major goal to prevent any false data injection or modification by malicious activities. One other challenging aspect is the scale of WSNs; these tiny wireless devices are deployed in large numbers and should produce in with low cost then import some constraints to capabilities and configurations of sensors such as power, memory, computational processor and physical tamper resistance [2, 3].

1.2 Problem Background

One of the recent subjects in computer network area is the wireless network that attracted much attention to it during last couple years. Especially when some new technology and standards were introduced to make it more reliable and stable Furthermore, make it possible to communicate with in more distances like 802.15.4 in wireless personal area network. As a result of those mention above, wireless sensor network was revealed. WSN can be defined as a group of sensors that consciously detected some physical measures from environment then through creating wireless networks with each other and communicating finally sent what are observed to a central node (Sink or Base Station) as a commander or administrator to calculating concluding result or sent out and executes necessary actions. At first, WSN just was used in military purpose, but now it’s going to take part in many industrial. Some of the WSN applications are: detecting fire in forest and another example is using WSN in monitoring and detection of leaking in gas, oil and water pipeline infrastructure. However, it is going to be used more and more in the future, so between these new technologies one of the most concerning matters is security of WSN from adversary goals. What we are going to research for this thesis is related to wireless sensor network and especially one sort of attacks, which called Byzantine attack. There are several kinds and categorization of attack in WSN. Some of them are similar to attack on other kinds of network and some other not and make WSN more vulnerable to adversaries. So the main subject here is Byzantine attack in the wireless sensor networks [4].

1.3 Problem Statement

Before we go deep in purpose and objective, it’s better to clearly have a problem definition. One of the most effective attacks on WSN is Byzantine, and it can be described as when one or several of nodes on the network compromised by an adversary from the outside of network. Those nodes had some delicate information of their own like the data from sensing the environment and also have some important information of network like shared keys, etc. so by compromising them the abuser can get access to those or by reprogramming and manipulating them can do malicious thing to network like dropping selective packets, sent wrong routing patch to other neighbors while did its regular jobs and reporting. In this situation, no one doubts about arbitrary of those nodes as then prevent of network services and in the worse, storyline makes network down.

1.4 Project Purpose

Due to the nature of wireless network, WSNs have much vulnerability led to variety of threads and attacks. It makes security as one of the most important elements in WSNs. Internal attacks are not considered as enough as they should be, so the main goal, here is to secure wireless sensor network, particularly in dealing with Black hole attack, which is originally a term of inside attack against routing protocol.

1.5 Project Objective

To approaching primary purposes of this thesis, we have done research in previous related works that are done in securing wireless sensor network, until now, comparing these methods and methodologies with each other and extract sufficient knowledge, then choose the best combination of them and perform some development and improvement, especially in main vulnerabilities and weakness to design a new novel Black hole resilient security mechanism with lower calculation and transmission rate for increasing power saving in life time of sensors and optimal performance. The result is a secure lightweight routing protocol for detecting and mitigating Byzantine attack. Based on problem statement, the following objectives have been formulated:

1. To do a review on security solutions in the wireless sensor network (WSN) against Black hole attack.
2. To present an improved security mechanism for one of the popular Byzantine attacks that performs better than existing mechanisms.
3. To implement proposed idea and security mechanism into one existing well-known protocol.
4. To simulate the presented secure protocol for achieving the expected results.
5. To evaluate provided results through data analysis and comparison with other protocols and talks about future related work in conclusion.

1.6 Project Question

Due to defined objectives in previous sections, five questions in follow section have been distinguished:

1. How to come with a good review of WSNs and different kinds of attacks in this area?
2. Why still there is no accepted global standard protocol for wireless sensor network and how choose a suitable security mechanism?
3. How to design and implement the resilient inside attack mechanisms without sacrificing power consumption and what is best option of well-known protocol?
4. What are requirements of simulations and how to provide them?
5. Is it really appropriate evaluation to provide data analysis of secure mechanisms against Byzantine attacks in WSNs and what could be our furtherer research steps?

1.7 Project Significance

The significance of this thesis is about every work that has been done, until now, is not completely secure against every kind of attack, and most of them focuses on outside attack and approach to good result. However, still there is an important gap in this way for inside attacks like Black hole attacks and there is no efficient method that can resist against Black hole attacks with the optimal provided result. Furthermore, previous techniques cannot apply to internal attacks because of some existing differences in algorithms. Even though, there are some offered methods like using binary search and accumulation signature technology but don’t be applied to real wireless sensor network's condition. So a novel Black hole resilient algorithm and method that can detect and as a result of that mitigate attack consequences by selecting the best route among Byzantine nodes and trusted nodes with setting cost of trustworthiness to each possible route from source to destination and further methods is proposed.

1.8 Project Scope

In this thesis first, brief information about WSNs, variety of Attacks and some previous works that have been done in this area is discussed. The rest of the thesis is about defined a network model and our presented method for detection and mitigation of Byzantine attack in WSNs. The identified scopes of research are limited to wireless sensor network is some specific features such as:

1. We have numerous nodes, which can be mobile or fix with using multi hop architecture as packet transferring system.
2. Only consist of most famous internal attacks in WSNs. However, it still takes more than a master thesis to include all of them so after some analysis it has been limited to just one well-known Byzantine attack, black hole attack, and left the rest for future works, which are discussed in last section of the thesis.
3. Due to limitation of resources, a real world experimental has been changed to simulation and extract demanded results like every other proper qualified work in this area.

1.9 Summary

In this chapter, the overall idea behind this project has been explained. Especially with glancing to objective's sections, main purpose of the thesis can be observed. Later chapters will discuss to uncover knowledge behind wireless networks and well-known proposed protocols in this area, and then talks about methodology for implementation of the project, show test result and analysis data of results. Finally, the summary of project and suggestion of future works is mention in the final chapter of this thesis.

REFRENCES

[1] Iqbal, M. and H.B. Lim. A cyber-physical middleware framework for continuous monitoring of water distribution systems. In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems. 2009. ACM.

[2] Uluagac, A.S., et al., Designing secure protocols for wireless sensor networks, in Wireless Algorithms, Systems, and Applications. 2008, Springer. p. 503-514.

[3] Akyildiz, I.F., et al., Wireless sensor networks: a survey. Computer networks, 2002. **38**(4): p. 393-422.

[4] Curtmola, R. and C. Nita-Rotaru, BSMR: byzantine-resilient secure multicast routing in multihop wireless networks. Mobile Computing, IEEE Transactions on, 2009. **8**(4): p. 445-459.

[5] Ahmed, A.A., H. Shi, and Y. Shang. A survey on network protocols for wireless sensor networks. In Information Technology: Research and Education, 2003. Proceedings. ITRE2003. International Conference on. 2003. IEEE.

[6] Driscoll, K., et al. The real byzantine generals. in Digital Avionics Systems Conference, 2004. DASC 04. The 23rd. 2004. IEEE.

[7] Challal, Y., et al., Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks. Journal of Network and Computer Applications, 2011. **34**(4): p. 1380-1397.

[8] Zhou, D. Security issues in ad hoc networks. In The handbook of ad hoc wireless networks. 2003. CRC Press, Inc.

[9] Capkun, S., L. Buttyán, and J.-P. Hubaux, Self-organized public-key management for mobile ad hoc networks. Mobile Computing, IEEE Transactions on, 2003. **2**(1): p. 52-64.

[10] Capkun, S., J.-P. Hubaux, and L. Buttyan, Mobility helps peer-to-peer security. Mobile Computing, IEEE Transactions on, 2006. **5**(1): p. 43-51.

[11] Eschenauer, L. and V.D. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security. 2002. ACM.

[12] Raya, M. and J.-P. Hubaux. The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. 2005. ACM.

[13] Van Der Merwe, J., D. Dawoud, and S. McDonald. Fully self-organized peer-to-peer key management for mobile ad hoc networks. In Proceedings of the 4th ACM workshop on Wireless security. 2005. ACM.

[14] Haas, Z.J., et al., Wireless ad hoc networks. 2002: Wiley Online Library.

[15] Zhou, L. and Z.J. Haas, Securing ad hoc networks. Network, IEEE, 1999. **13**(6): p. 24-30.

[16] Ben Salem, N., et al., Node cooperation in hybrid ad hoc networks. Mobile Computing, IEEE Transactions on, 2006. **5**(4): p. 365-376.

[17] Talzi, I., et al. PermaSense: investigating permafrost with a WSN in the Swiss Alps. In Proceedings of the 4th workshop on Embedded networked sensors. 2007. ACM.

[18] Buttyán, L. and J.-P. Hubaux. Enforcing service availability in mobile ad-hoc WANs. In Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing. 2000. IEEE Press.

[19] Hu, Y.-C., A. Perrig, and D.B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 2005. **11**(1-2): p. 21-38.

[20] Marti, S., et al. Mitigating routing misbehavior in mobile ad hoc networks. In International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking. 2000.

[21] Aad, I., J.-P. Hubaux, and E.W. Knightly. Denial of service resilience in ad hoc networks. In Proceedings of the 10th annual international conference on Mobile computing and networking. 2004. ACM.

[22] Papadimitratos, P. and Z.J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS). 2002.

[23] Papadimitratos, P. and Z.J. Haas. Secure data transmission in mobile ad hoc networks. In Proceedings of the 2nd ACM workshop on Wireless security. 2003. ACM.

[24] Avramopoulos, I., et al. Highly secure and efficient routing. In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. 2004. IEEE.

[25] Awerbuch, B., et al. An on-demand secure routing protocol resilient to byzantine failures. In Proceedings of the 1st ACM workshop on Wireless security. 2002. ACM.

[26] Stallings, W., Cryptography and network security, principles and practices, 2003. Practice Hall.

[27] Zhou, L. and Z.J. Haas, Securing ad hoc networks. Network, IEEE, 1999. 13(6): p. 24-30.

[28] Ertaul, L. and N. Chavan. Security of ad hoc networks and threshold cryptography. In Wireless Networks, Communications and Mobile Computing, 2005 International Conference on. 2005. IEEE.

[29] Schneier, B., Beyond fear: Thinking sensibly about security in an uncertain world. 2003: Springer.

[30] Qian, L., N. Song, and X. Li, Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach. Journal of network and computer applications, 2007. 30(1): p. 308-330.

[31] Awerbuch, B., et al. An on-demand secure routing protocol resilient to byzantine failures. In Proceedings of the 1st ACM workshop on Wireless security. 2002. ACM.

[32] Hu, Y.-C., A. Perrig, and D.B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM workshop on Wireless security. 2003. ACM.

[33] Perkins, C.E. and P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Computer Communication Review, 1994. 24(4): p. 234-244.

[34] Das, S.R., E.M. Belding-Royer, and C.E. Perkins, Ad hoc on-demand distance vector (AODV) routing. 2003.

[35] Michiardi, P. and R. Molva. A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad hoc networks. in WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks. 2003.

[36] Hashmi, S. and J. Brooke. Authentication mechanisms for mobile ad-hoc networks and resistance to sybil attack. in Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on. 2008. IEEE.

[37] Douceur, J.R., The sybil attack, in Peer-to-peer Systems. 2002, Springer. p. 251-260.

[38] Hu, Y.-C., A. Perrig, and D.B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 2005. 11(1-2): p. 21-38.

[39] Johnson, D.B., D.A. Maltz, and J. Broch, DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 2001. 5: p. 139-172.

[40] Hu, Y.-C., D.B. Johnson, and A. Perrig, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 2003. 1(1): p. 175-192.

[41] Perrig, A., et al. Efficient and secure source authentication for multicast. in Network and Distributed System Security Symposium, NDSS. 2001.

[42] Hu, Y.-C., A. Perrig, and D.B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. 2003. IEEE.

[43] Sanzgiri, K., et al. A secure routing protocol for ad hoc networks. in Network Protocols, 2002. Proceedings. 10th IEEE International Conference on. 2002. IEEE.

[44] Zapata, M.G., Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 2002. 6(3): p. 106-107.

[45] Papadimitratos, P. and Z.J. Haas. Secure link state routing for mobile ad hoc networks. in Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on. 2003. IEEE.

[46] Haas, Z.J. and M.R. Pearlman, The performance of query control schemes for the zone routing protocol. IEEE/ACM Transactions on Networking (TON), 2001. 9(4): p. 427-438.

[47] Awerbuch, B., et al., ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information and System Security (TISSEC), 2008. **10**(4): p. 6.

[48] Theodorakopoulos, G. and J.S. Baras, on trust models and trust evaluation metrics for ad hoc networks. Selected Areas in Communications, IEEE Journal on, 2006. 24(2): p. 318-328.

[49] Papadimitratos, P. and Z.J. Haas. Secure routing for mobile ad hoc networks. in Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS). 2002.

[50] Kschischang, F.R., B.J. Frey, and H.-A. Loeliger, Factor graphs and the sum-product algorithm. Information Theory, IEEE Transactions on, 2001. 47(2): p. 498-519.

[51] Liu, D., P. Ning, and W.K. Du. Attack-resistant location estimation in sensor networks. in Proceedings of the 4th international symposium on Information processing in sensor networks. 2005. IEEE Press.

[52] Intanagonwiwat, C., R. Govindan, and D. Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. in Proceedings of the 6th annual international conference on Mobile computing and networking. 2000. ACM.

[53] Yu, Y., R. Govindan, and D. Estrin, Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks, 2001, Citeseer.

[54] Karp, B. and H.-T. Kung. GPSR: Greedy perimeter stateless routing for wireless networks. in Proceedings of the 6th annual international conference on Mobile computing and networking. 2000. ACM.

[55] Ye, F., et al. A scalable solution to minimum cost forwarding in large sensor networks. in Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on. 2001. IEEE.

[56] Heinzelman, W.R., A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. in System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on. 2000. IEEE.

[57] Braginsky, D. and D. Estrin. Rumor routing algorthim for sensor networks. in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications. 2002. ACM.

[58] Haas, Z.J., J.Y. Halpern, and L. Li. Gossip-based ad hoc routing. in INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. 2002. IEEE.

[59] Xu, Y., J. Heidemann, and D. Estrin. Geography-informed energy conservation for ad hoc routing. in Proceedings of the 7th annual international conference on Mobile computing and networking. 2001. ACM.

[60] Marti, S., et al. Mitigating routing misbehavior in mobile ad hoc networks. in International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking. 2000.

[61] Buchegger, S. and J.-Y. Le Boudec. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. in Parallel, Distributed and Network-based Processing, 2002. Proceedings. 10th Euromicro Workshop on. 2002. IEEE.

[62] Zhou, H., M.W. Mutak, and L.M. Ni. Secure autoconfiguration and public-key distribution for mobile ad-hoc networks. in Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on. 2009. IEEE.

[63] Perrig, A., et al., SPINS: Security protocols for sensor networks. Wireless networks, 2002. 8(5): p. 521-534.

[64] Cavalli, A. and J.-M. Orset. Secure hosts auto-configuration in mobile ad hoc networks. in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. 2004. IEEE.

[65] Marti, S., et al. Mitigating routing misbehavior in mobile ad hoc networks. in International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking. 2000.

[66] Acharya, A., A. Misra, and S. Bansal. MACA-P: a MAC for concurrent transmissions in multi-hop wireless networks. in Pervasive Computing and Communications, 2003.(PerCom 2003). Proceedings of the First IEEE International Conference on. 2003. IEEE.

[67] Pickholtz, R.L., L.B. Milstein, and D.L. Schilling, Spread spectrum for mobile communications. Vehicular Technology, IEEE Transactions on, 1991. 40(2): p. 313-322.

[68] Blum, L., M. Blum, and M. Shub, A simple unpredictable pseudo-random number generator. SIAM Journal on computing, 1986. 15(2): p. 364-383.

[69] Jiang, T. and J.S. Baras. Autonomous Trust Establishment1. in Proceedings INOC. 2005.

[70] Kamvar, S.D., M.T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. in Proceedings of the 12th international conference on World Wide Web. 2003. ACM.

[71] Issariyakul, T., Introduction to network simulator NS2. 2012: Springer Science+ Business Media.

[72] Mackar, J. and S. Corson, RFC 2501,“. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, IETF, 1999.