International Journal of Information Processing, 7(2), 59-68, 2013
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Multiple Domain Secure Routing for Wireless Sensor Networks

Lata B T, Jansi P K R, Shaila K, SivaSankari H, D N Sujatha, Venugopal K R[a], and L M Patnaik[b]

[a]University Visvesvaraya College of Engineering, Bangalore, India, Contact: lata_bt@yahoo.co.in

[b]Indian Institute of Science, Bangalore, India

Secure Transmission of data packets in Wireless Sensor Networks is an important area of Research. There is a possibility of an attacker creating security holes in the network. Hence, network security and reliability can be achieved by discovering random multiple paths using multiple domains and forwarding data packets from the source node to the destination node. We have designed, Multiple Domain Routing with Overlap of Nodes (MDRON) and Multiple Domain Routing Without Overlap of Nodes (MDRWON) algorithms, in which packets follow multiple paths simultaneously. The Special node algorithm searches the node which has maximum power and these nodes are used for transferring the packet from one domain to another domain. Simulation results using MATLAB shows that performance is better than Purely Random Propagation (PRP) and Non Repetitive Random Propagation(NRRP) Algorithms.

Keywords : Multiple Domain, Random Routing, Special nodes, Wireless Sensor Networks.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of a large number of ultra-small, low-cost, battery-powered devices that have limited energy resources, computation, memory and communication capabilities. WSNs are often deployed in a vast terrain to detect events of interest and deliver data reports over wireless path to the sink. WSNs are used in environment monitoring, military applications, home appliance management, commercial applications, *etc.*.

The major services of security are: Confidentiality, access control, authentication, non-repudiation and integrity. *Confidentiality* : It means the data to be transmitted should be protected from passive attacks. *Access Control* : It is the capability to control the access to host systems through the communication links. *Authentication* : It assures that the communication is established between the authentic user. It provides confidence in the identity of the entities connected and assures that the received data is from the claimed source. *Nonrepudiation* : It provides the proof that the message was sent or received from the specified device. *Integrity* : It assures that the received data is exactly the same as it was sent by the authorized entity.

Even in the presence of security protocols, the adversaries are able to break the cipher text and find the plain text. Data security is essential for critical applications to work in hostile environments. It is easy for the attackers to inject malicious data messages or alter the content of legitimate messages during hop forwarding of data, due to the wireless environment in sensor networks. Thus, in sensor network communication, it is essential for authentication mechanisms to ensure that data from a valid source is not altered during transit. In this paper, we have focused on node compromise attack.

Motivation : Data packets are usually forwarded from one node to another using single or multiple hops in WSNs. The adversary observes the traffic during routing

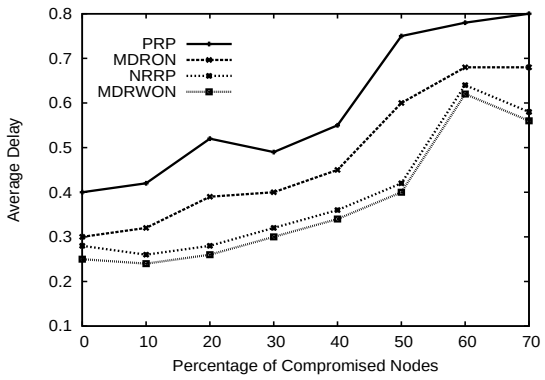

Figure 4. Average Delay Vs. Compromised Nodes.

node algorithms as discussed in Algorithm 1. Random path includes special node in each domain, which in turn enhances the packet delivery ratio as compared with PRP and NRRP. Multiple domains are not considered in PRP and NRRP. We have proposed the algorithms for both single and multiple domains. The result for special node selection algorithm is available in Table 1. Comparison of PRP, MDRON, NRRP and MDRWON is shown in Figure 1. The variation of packet drop for different number of compromised nodes in the network is shown in Figure 1. MDRON and MDRWON algorithms results better packet delivery ratio, as compared with PRP and NRRP.

In Figure 2, when the percentage of the number of compromised nodes increase, the packet drop increases gradually. In MDRON, there is a chance of overlapping of nodes. In MDRWON, overlapping of nodes is avoided, hence, the packet drop reduces by 2% in MDRWON as compared with MDRON. The packet delivery ratio decreases proportionately with the increase in the percentage of the number of compromised nodes as observed in Figure 2. The packet delivery ratio decreases by 8% in MDRON compared with MDRWON. Correspondingly, the throughput of the network reduces gradually with increase in the percentage of compromised nodes as observed in Figure 3. The average delay of the packets reaching the destination increases with increase in the number of compromised nodes. The delay of the packets reaching the destination is reduced in MDRON and MDRWON by 10% and 2% compared with PRP and NRRP respectively as shown in Figure 4.

9. CONCLUSIONS

Security is an important issue in WSNs. This paper proposes a Secure Multiple Domain Routing for Wireless Sensor Networks, that consists of a special node, in each domain, which helps in establishing secure communication. The algorithm discovers the route from one domain to another domain and within the domain which minimizes the effect of node compromise. Here, We are communicating through special nodes, which inturn enhances the delivery ratio for multiple domains, as compared with previous algorithms, decreases packet drop that is caused by the compromised nodes, and increases throughput. Numerical results demonstrates that the performance is better interms of reduced packet drop, increases packet delivery and throughput by avoiding the node from compromising with the adversary.

REFERENCES

1. Yun Zhou and Yuguang Fang, Securing Wireless Sensor Networks: A Survey, *IEEE Communications,* 10(3):6-28, 2008.
2. Chris Karlop and David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, *Proceedings of the First IEEE Communications, Elsevier,* pages 113-127, 2003.
3. Chih-Yung Chang, Chao-Tsum Chang and Shih-Chief Lee, "Active Route- Guiding Protocol for Resisting Obstacles in Wireless Sensor Networks," *IEEE Transactions on Vehicular Technology,* 59(9):4425-4442, Nov 2010.
4. P Samundiswary, D Sathian and P Dananjayan, "Secured Greedy Perimeter Stateless Routing for Wireless Sensor Networks," *International Journal of Ad hoc, Sensor and Ubiquitous Computing (IJASUC),* 1(2):9-20, June 2010.

5. Wenjing Lou and Younggoo Kwon, H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks, *IEEE Transactions on Vehicular Technology,* 55(4):1320-1330, July 2006.
6. Feilong T, Minyi G, Minglu L, Aho-Li W, and Mianxiong D, Secure Routing for Wireless Mesh Networks in Pervasive Environments, *International Journal of Intelligent Control and Systems,* 12(4):293-306, December 2007.
7. Md. Abdul Hamid, Md. Mamun-Or-Rasid and Choong Seon Hong, "Routing Security in Sensor Networks: HELLO Flood Attack and Defense, *In Proceedings of The International Conference on Next-Generation Wireless Systems,* ICNEWS 2006.
8. T Shu, M Krunz, S Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," *IEEE Transactions on Mobile Computing,* 9(7):941-954, July 2010.
9. Tian Cheng li, Ninghui Li, Jian Zhang and Ian Molloy, Slicing: A New Approach to Privacy Preserving Data Publishing, *IEEE Transactions on Knowledge and Data Engineering,* 24(3), March 2012.
10. Yihong Zang, Johnson P Thomas, Gheorghita Chinea, Mathews Thomas and Salaheddin Darwish, "Secure Sector Based Bi-Path Clustering and Routing Protocol for WSNs," *IEEE Computer Society, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,* pages 777-784, 2012.
11. Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhing Chen and Xuemin Shen, "Secure and Energy-Efficient Disjoint Multipath Routing for WSNs," *IEEE Transactions on Vehicular Technology,* 16(7):3255-3265, September 2012.
12. Min-Ho Park, Young-Hoon Park, Han-YounJeong and Seung-Woo Seo, "Secure Multiple Multicast Services in Wireless Networks," *IEEE Transactions on Mobile Computing,* pp(99):1-13, June 2012.
13. Asmae Blilat, Anas Bouayad, Nour Chaoui, Mohammed Ghazi, "Wireless Sensor Network:Security Challenges," *IEEE Conference on Network Security and Systems (JNS2),* pages 68-72, April 2012.

Lata B T is an Assistant Professor in the Department of Computer Science and Engineering at University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. She obtained her B.E degree in Computer Science and Engineering from Karnatak University, Dharwad, and M.Tech. degree in Computer Network Engineering from Visveswaraiah Technological University, Belgaum. She is pursuing her Ph.D degree in the area of Wireless Sensor Networks in Bangalore University, Bangalore. Her research interest is in the area of Sensor Networks.

Jansi P K R obtained her M.E in the Department of Computer Science and Engineering at University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. Her research interest is in the area of Sensor Networks.

Shaila K is an Professor and Head in the Department of Electronics and Communication Engineering at Vivekananda Institute of Technology, Bangalore, India. She obtained her B.E in Electronics and M.E degrees in Electronics and Communication Engineering from Bangalore University, Bangalore. She obtained her Ph.D degree in the area of Wireless Sensor Networks in Bangalore University. Her research interest is in the area of Sensor Networks, Adhoc Networks and Image Processing.

H Sivasankari is an Associate Professor and Head in the Department of Information Science and Engineering at AMC College of Engineering, Bangalore, India. She obtained her B.E in Electronics and Instrumentation Engineering and M.E degree in Computer Science and Engineering. She is presently pursuing her

Ph.D programme in the area of Wireless Sensor Networks in Jawaharlal Nehru Technological University. Her research interests are in the area of Sensor Networks.

D N Sujatha is an Professor and Head in the Department of Computer Applications at B M S College of Engineering, Bangalore, India. She obtained her B.Sc and MCA degrees from Mysore University, Mysore. She obtained her Ph.D degree in the area of Computer Networks from Bangalore University. Her research interest is in the area of Sensor Networks and Computer Networks.

Venugopal K R is currently the Principal, University Visve svaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D in Economics from Bangalore University and Ph.D in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 39 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ *etc.*. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 350 research papers to his credit. His research interests include Computer Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

L M Patnaik is an Honorary Professor, Indian Institute of Science, Bangalore. He was the Former Vice Chancellor, Defense Institute of Advanced Technology, Pune, India. He was a Professor since 1986 with the Department of Computer Science and Automation, Indian Indian Institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Journals and referred International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. His areas of research interest have been parallel and distributed computing, mobile computing, CAD for VLSI circuits, Soft Computing and Computational Neuroscience.