International Journal of Information Processing, 6(4), 27-41, 2012
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Trust Based Model for Secure Key Distribution and Routing in Mobile Wireless Sensor Networks

Thejaswini S[a], N R Sunitha[b], B B Amberker[c]

[a]Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India, Contact: thejaswinis@sit.ac.in

[b]Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India, Contact: nrsunitha@sit.ac.in

[c]Department of Computer Science and Engineering, National Institute of Technology, Warnangal, AndraPradesh, India, Contact: bba@nitw.ac.in

As the use of mobile Wireless Sensor Networks(WSNs) spreads beyond personal networks to practical military applications, addressing security issues becomes extremely important in this area. However, mobile networks are more susceptible to malicious behavior. Thus, an effective node evaluation mechanism can prevent malicious nodes from initiating attacks and tampering the data communication process in the networks. In Wireless Sensor Network (WSN), different roles can be associated with sensor nodes. However, depending on the application a node can be dedicated to a particular special role. This paper explores a dynamic role based trust model for key distribution and route selection mechanism for WSN. In this approach we have recognized the different roles of sensor such as Packet Forwarding, Data Aggregation and Time Synchronization. Each node maintains a reputation table which holds reputation values for different roles of all neighboring sensors and using this table data is routed to destination by evaluating the trustworthiness of the sensors based on different roles. In this paper, an efficient and dynamic trust based symmetric key distribution mechanism is proposed for secure communication between nodes in a densely populated mobile WSN and trust model for routing is proposed which is reliable, scalable and has simple trust computation for different roles. Using this model secure routing can be furnished by detecting malicious and faulty nodes w.r.t different roles.

Keywords : Data Aggregation, Pair-Wise Key, Reputation, Time Synchronization, Trust.

1. INTRODUCTION

In recent decades, WSNs provide many benefits to mobile users and devices and have attracted a lot of attention due to their extensive applications in both military and civilian applications. With the rapid technology development of wireless communication and Micro-Electro-Mechanical Systems (MEMS) during these several decades [1-3], the WSN offers a efficient solution in a great variety of applications [4]: such as reconnaissance, disaster relief, intelligent transportation, surveillance, environmental monitoring, health care, target tracking, industry control, intelligent green aircrafts, smart roads and more. As applications gain more importance, security issues have become a hot research topic. However, they pose a number of non-trivial challenges for wireless services. The security is one such challenging and crucial issue in WSN, due to various reasons such as: (i) Sensor nodes are often deployed in open and hostile environments without physical protection. Hence, sensor network is easily vulnerable to active and passive attacks [5]. (ii) WSNs are functioned with limited computing power, limited energy resources, limited communications bandwidth, limited communication range and limited storage resources. Due to this reasons, secure communication is more complex task in WSN [6].

work. Once the nodes energy level reduces to below specified threshold value even though the node is trustable it will be further not used in the network. Because if the complete energy is used, the network may face energy-hole problem which affects the reliable communication between nodes in the network. Hence, to maintain secure and reliable communication it is necessary to consider energy level of each and every node in the network.

Table 1
Trust Table of a Sensor

NodeId	Sensor's Role	Trust Value	Time Stamp

4. CONCLUSIONS

Since the sensor position is not static, providing security for a densely populated mobile sensor network is a challenging task. However, in almost all the existing schemes the base station distributes the key to the sensors for their secure communication. If the sensors are at long distance from the base station, the secure communication becomes a tedious process which requires more number of request and reply message exchanges between the sensors and the base station. Hence, resulting with several flaws in the network performance such as: heavy communication and storage overhead, more energy consumption, reduction in network life time *etc.*. Hence, in the proposed scheme we have addressed a neighbor based pair-wise key distribution and role based dynamic trust route selection to overcome the flaws occurred in the existing schemes. Thus, providing the advantages related with the following issues:

- The key distribution load is reduced on the base station, since each and every node has the ability to distribute the key to requested sensor.
- Since the key is dynamically generated by the sensor, the storage overhead is reduced.
- The number of transmissions required while forwarding the request and reply messages to and from the base station is reduced.
- Malicious nodes are identified and are eliminated based on the sensors role for performing the relevant task in the network.
- In the routing process, if multiple paths exist between the sensors then the most trustworthy nodes are selected.
- Simple computation of trust based on the sensors role reduces the energy consumption.

5. FUTURE ENHANCEMENT

There is potential for improvements to our proposed scheme w.r.t following issues:

- Trustworthiness of sensor can be evaluated by identifying other different role of sensors such as localization, target tracking *etc.*.
- The proposed scheme can be employed in the real world densely populated wireless sensor network.

ACKNOWLEDGEMENT

We thank AICTE for funding this research work F.No: 8023/BOR/RID/RPS-16/2008-09.

REFERENCES

1. K Rmer and F Mattern. The Design Space of Wireless Sensor Networks, *In: Proceedings of IEEE Wireless Communications* 11(6):54-61, December 2004.
2. Hee Wan Kim, Hee Suk Seo, Sun Ho Hong, Chul Kim. Modeling of Energy- Efficient Applicable Routing Algorithm in WSN, *International Journal of Digital Content Technology and its Applications*, 4(5):13-22, 2010.
3. Akyildiz I F, SuWL, Sankarasubramaniam Y, Cayirci E. A survey on Sensor Networks, *In Proceedings of IEEE Communications Magazine*, 40(8):102-114, 2002.

4. QI Xiao-gang, QIU Chen-xi. An Improvement of GAF for Lifetime Elongation in Wireless Sensor Networks, *Journal of Convergence Information Technology*, 5(7):112-119, 2010.
5. Yi Cheng, Dharma P Agrawal. An Improved Key Distribution Mechanism for Large-Scale Hierarchical Wireless Sensor Networks, *Ad Hoc Networks*, 5:35–48, 2007.
6. Mi Wen, Yan-Fei Zheng, Wen-jun Ye, Ke-Fei Chen, Wei-Dong Qiu. A Key Management Protocol with Robust Continuity for Sensor Networks, *In: Proceedings of the Computer Standards and Interfaces*, 31, pages 642–647, 2009.
7. H Chan and A Perrig. Security and Privacy in Sensor Networks, *In: Proceedings of the IEEE Computer*, 36(10):103–105, 2005.
8. D Carman, P Kruus, B Matt. Constraints and Approaches for Distributed Sensor Network Security. *Technical Report 00-010, NAI Labs*, pages 01-1-010, September 2000.
9. C Kuo, M Luk, R Negi and A Perrig. Message-in-a-Bottle: Userfriendly and Secure Key Deployment for Sensor Nodes, *In Proceedings of the Fifth International Conference on Embedded Networked Sensor Systems (SenSys07), ACM, New York, NY, USA*, pages 233–246, 2007.
10. P Resnick and R Zeckhauser. Trust among Stranger in Internet Transactions: Empirical Analysis of Ebays Reputation System, *In Proceedings of NBER workshop on Empirical Studies if Electronic Commerce*, 2000.
11. L Xiong and L Liu. A Reputation-based Trust Model for Peer-to-Peer Ecommerce Communities, *In: proceedings of the IEEE conference on Ecommerce*, 2003.
12. A Rahbar and O Yang. Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing, *IEEE Transactions on Parallel and Distributed Systems*, 18(4):460–473, 2007.
13. S Camtepe and B Yener. Key Distribution Mechanisms for Wireless Sensor Networks: A Survey, *Technical report, Rensselaer Polytechnic Inst.,* 2005.
14. Y Xiao, V Rayi, B Sun, X Du, F Hu, and M Galloway. A survey of Key Management Schemes in Wireless Sensor Networks, *In proceedings of the Computer Communications, Special Issue on Security on Wireless Ad hoc and Sensor Networks, Elsevier North-Holland, Inc., New York, NY, USA,* pages 2314–2341, 2007.
15. A Barati, M Dehghan, H Barati, and A Mazreah. Key Management Mechanisms in Wireless Sensor Networks, *In Proceedings of the second International Conference on Sensor Technologies and Applications (SENSORCOMM08), IEEE Computer Society, Washington, DC, USA,* pages 81–86, 2008.
16. J Zhang and V Varadharajan. Wireless Sensor Network Key Management Survey and Taxonomy, *North-Holland, USA,* pages 315–326, 2009.
17. Chan H and Perrig A. PIKE: Peer Intermediaries for Key Establishment in Sensor Networks, *In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 05), Miami, FL, USA,* pages 524–535, March 2005.
18. Eschenauer L and Gligor B D. A Key Management Scheme for Distributed Sensor Networks, *In Proceedings of the 9th ACM Conference on Computer and Communication Security, Washington D C, USA,* pages 41–47, 2002.
19. Y Cheng and D P Agrawal. Efficient Pairwise Key Establishment and Management in Static Wireless Sensor Networks, *In Proceedings of the Second IEEE International Conference on Mobile Ad hoc and Sensor Systems, Washington, DC,* November 7-10, 2005.
20. Chan H and Perrig A. Random Key Predistribution Schemes for Sensor Networks, *In Proceedings of the IEEE Symposium on Security and Privacy*, pages 197–213, May 2003.
21. Liu D and Ning P. Establishing Pair-Wise Keys in Distributed Sensor Networks, *In Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington, DC ACM Press*, pages 197–213, 2003.
22. Blom R. Theory and Application of Cryptographic Techniques, *In Proceedings of the Eurocrypt 84 workshop on advances in cryptology. Berlin: Springer*, pages 335–338, 1985.
23. Lee J and Stinson D R. Deterministic Key Predistribution Schemes for Distributed Sensor Networks, *In Proceedings of the ACM symposium on Applied Computing, Lecture Notes in Computer Science*, pages 294–307, 2005.
24. Nathan Lewis, Noria Foukia, and Donovan G Govan. Using Trust for Key Distribution and Route Selection in Wireless Sensor Networks, *Network Operations and Management Symposium, NOMS 2008. IEEE*, pages 787-790, 2008.

25. S Buchegger and J L Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad hoc Networks, *In Proceedings of the Tenth Euromicro Workshop Parallel, Distr. Netw.-based Process*, pages 403–410, 2002.
26. Q He, O D Wu, P Khosla and SORI. A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks, *In Proceedings of the IEEE Conference on Wireless Communications and Networking*, 2004.
27. S D Kamvar, M T Schlosser and H Garcia-Molina. The Eigen Trust Algorithm for Reputation Management in P2P Networks, *In Proceedings of the 12th International World Wide Web Conference, Budapest, Hungary,* pages 640–651, 2003.
28. N Li, J Mitchell and R T. A Role-based Trust-Management Framework, *In Proceedings of the Third DARPA Inform. Surviv. Conf. Exposition (DISCEX03)*, pages 201–212, April 2003.
29. Z Liu, A W Joy and R A Thompson. A Dynamic Trust Model for Mobile Ad hoc Networks, *In Proceedings of the Tenth IEEE International Workshop Future Trends Distr. Comput. Syst. (FTDCS04), Suzhou, China,* pages 80–85, May 2004.
30. P Michiardi and R Molva. Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad hoc Networks, *In Proceedings of the Sixth IFIP Commun. Multimedia Secur. Conference, Portorosz, Slovenia,* pages 107–121, 2002.
31. T G Papaioannou and G D Stamoulis. Effective Use of Reputation of Peer-to-Peer Environments, *In Proceedings of the IEEE/ACM CCGRID, GP2PC workshop, Chicago, USA* April 2004.
32. A A Pirzada and C McDonald. Establishing Trust in Pure Ad-hoc Networks, *In Proceedings of the 27th Conf. Australasian Computer Sci., ACM Intl Conf. Proc. Series, Dunedin, New Zealand,* pages 47–54, 2004.
33. Y Wang and J Vassileva. Trust and Reputation Model in Peer-to-Peer Networks, *In Proceedings of the Third Intl Conf. Peer-to-Peer Comput. (P2P03), Linkoping, Sweden*, pages 150–157, Sept. 2003.
34. P Chatterjee, I SenGupta and S K Ghosh. A Trust Based Clustering Framework for Securing Ad Hoc Networks, *In Proceedings of the ICISTM 2009, Ghaziabad, India,* pages 313–324, 2009.
35. Carlos R Perez-Toro, Rajesh K Panta and Saurabh Bagchi. RDAS: Reputation- based Resilient Data Aggregation in Sensor Network, *IEEE Secon 2010 Publications*, 2010.
36. S Marti, T Giuli, K Lai and M Baker. Mitigating Routing Misbehavior in Mobile Ad hoc Networks, *In Proceedings of the 6th ACM/IEEE International Conference on Mobile Computing and Networking*, pages 255–265, 2000.
37. R Roman, J Zhou and J Lopez. Applying Intrusion Detection Systems to Wireless Sensor Networks, *In Proceedings of the Consumer Communications and Networking Conference*, pages 640–644, 2006.
38. Argyroudis P G and OMahony D. Towards Flexible Trust in Wireless Sensor, *In Proceedings of the 10th IEEE Symposium on Computers and Communications*, Pages 421–426, 2005.
39. Haiguang Chen. Task-based Trust Management for Wireless Sensor Networks, *International Journal of Security and Its Applications* 3(2), April 2009.
40. Taghikhaki Z, Meratnia N and Havinga. Energy Efficient Trust based Data Aggregation in Wireless Sensor Networks, *In Proceedings of the Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference*, pages 584–589, April 2011.
41. A Josang and R Ismail. The Beta Reputation System, *In Proceedings of the 15th Bled Conf. Electronic Commerce*, pages 41–50, 2002.
42. Jason Hill. System Architecture for Wireless Sensor Networks, *Ph.D. Thesis, UC Berkeley,* May 2003.
43. Shujuan Chen, Adam Dunkels, Fredrik Osterlind, Thiemo Voigt and Mikael Johansson. Time Synchronization for Predictable and Secure Data Collection in Wireless Sensor Networks, *In Proceedings of the Sixth Annual Mediterranean Ad hoc Networking Workshop (Med-Hoc-Net 2007)*, 2007.
44. A Salhieh, J Weinmann, M Kochhal and L Schwiebert. Power Efficient Topologies for Wireless Sensor Networks, *In Proceedings of the ICPP01, Valencia, Spain,* pages 156–163, Sept. 2001.
45. M Khan, G Pandurangan and B Bhargava. Energy-Efficient Routing Schemes for Wireless Sensor Networks, *A Tech. Rep., CSD TR 03-013, Department of Computer Science, Purdue University,* July 2003.

46. W Ye, J Heidemann and D Estrin. An Energy-Efficient MAC Protocol for Wireless Sensor Networks, *In proceedings of the INFOCOM 2002, New York,* pages 1567–1576, June 2002.
47. T V Dam and K Langendoen. An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks, *In Proceedings of the SenSys03, Los Angeles,* pages 171–180, Nov. 2003.
48. G Lu, B Krishnamachari and C Raghavendra. An Adaptive Energy-Efficient and Low-Latency MAC for Data Gathering in Sensor Networks, *In Proceedings of the International Workshop on Algorithms for Wireless, Mobile, Ad hoc and Sensor Networks (WMAN 04)*, April 2004.
49. W Heinzelman, A Chandrakasan and H Balakrishnan. Energy-Efficient Communication Protocols for Wireless Microsensor Networks, *In Proceedings of the Hawaian Intl Conf. on Systems Science*, Jan. 2000.
50. W Heinzelman, J Kulik and H Balakrishnan. Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, *In Proceedings of the 5th ACM/IEEE Mobicom Conference, Seattle, WA,* Aug. 1999.