International Journal of Information Processing, 8(4), 1-11, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Identification of Parameters and Trust Factors for Trust Based Secure Communication in Wireless Sensor Networks

Geetha V[a], K Chandrasekaran[a]

[a]Department of Information Technology, National Institute of Technology Karnataka, Surathkal, D.K, 575 025, India, Contact:geethav.nitk@gmail.com, kchnitk@gmail.com

Trust in wireless sensor networks are an essential feature to detect various kind of attacks such as blackhole, sinkhole and greyhole attack. To develop an efficient trust management system, it is required to identify various parameters which need to be observed to detect different type of attacks. This paper proposes and identifies various parameters which in general influences on trust management in wireless sensor network. Based on identified parameters we also identify various trust factors to be considered in any wireless sensor network for secure communication. As a case study we have taken Low Energy Adaptive Cluster Head protocol to analyze the effect of proposed set of parameters. Experiments are conducted using Network Simulator NS2.

Keywords : Low Energy Adaptive Cluster Head Protocol(LEACH), Trust Factors, Trust Management, Trust Parameters, Wireless Sensor Networks.

1. INTRODUCTION

The Wireless Sensor Networks (WSN) are more prone to various kind of attacks as the nodes are deployed in an open environment. The traditional cryptographic techniques are not sufficient to detect various kind of attacks. The trust based approaches are proven good results in the areas of social networks, peer-to-peer networks and mobile ad-hoc networks. The resource constraint wireless sensor network, needs sophisticated methods to manage resources and provide efficient mechanism for detection of various kinds of attack.

Most of the researchers provided mechanism for identifying or detecting single type of attack in wireless sensor network. Our approach is to identify various parameters, where monitoring on values of these parameters, the attacks on various fields can be detected and further corrective measures can be taken based on trust factors in trust management system.

In wireless sensor network, the routing is the major area where most of the interactions happens for finding routes and sending sensed data to sink node or base station. Hence, it is essential to have trust management at routing layer to identify various kind of attacks. Even though the attacks such as jamming attack are possible at other layers, the solutions for such kind of attack does not comes under trust management. As a result, our focus is on routing layer for identifying various parameters and trust factors for secure communication in wireless sensor network.

Section 2 provides related work, Section 3 explains trust in wireless network and Section 4 explains our proposed work for identifying parameters which influences trust values in wireless sensor networks. Section 5 explains our proposed work for identifying trust factors for trust management to provide secure communication. Section 6 provides the results of simulation and discussions. Paper is concluded in Section 7 followed by reference.

2. RELATED WORK

Wireless sensor networks are more vulnerable to attacks as the nodes are deployed in an open environment. The researchers proposed sev-

Table 3
Parameters Values for Simulation in Each Cluster Head

Parameter	**CH1**	**CH2**	**CH3**	**CH4**	**CH5**
$P_{data}(t)$	0	31.6	25.00	25.00	25.00
$P_{fwd}(t)$	0	358	319	350	318

Table 4
Parameters Values with Simulation Time

Parameter	**Time: 100**	**Time: 200**	**Time: 300**	**Time: 400**	**Time: 500**
$P_{br}(t)$	46	28	40	12	14
$P_{rt}(t)$	46	28	40	12	14
$P_{av}(t)$	99	99	99	62	52

Table 3 and 4 show the observation of parameters in LEACH protocol, where the cluster head 1 is malicious node, which collects all data and drops the packets. By observing on $P_{fwd}(t)$, we can see that the number of packets forwarded by the cluster head 1 is zero. For data stealthiness, cluster head 2 is assumed to be having more nodes in it which acts as stealthy attack. As a result the aggregation value at cluster head varies depending on the stealthiness of node. $P_{br}(t)$ and $P_{rt}(t)$ shows that as the simulation time increases the number of broadcast packet decreases as the number of nodes available in the network goes down based on energy dissipation.

The experiment results concludes that building trust management by considering the proposed parameters may further help to identify various attacks on WSN. The parameters just provides values for various interaction. Further evaluation of these parameter values must lead in obtaining values for trust factors.

6. CONCLUSIONS

The trust in wireless sensor network depends on the observed behaviour of a node by its neighbour node. To ensure trustworthy network, it is not sufficient to observe one or two parameters like communication, or data. We have identified total six parameters which influences on trust in wireless sensor network. As a case study, LEACH protocol is considered for analysing the effect of parameters on wireless sensor networks. The trust value calculation on observing these parameters further improves the identification of various kind of attacks. We have also identified trust factors for trust management system to provide secure communication in wireless sensor networks. As a future work trust model can be built to observe the proposed parameters and evaluate trust factors to ensure the detection of various attacks. This is an ongoing work related to trust based secure communication in wireless sensor networks.

REFERENCES

1. Vinod Kumar Jatav, Meenakshi Tripathi, M S Gaur and Vijay Laxmi. Wireless Sensor Networks: Attack Models and Detection, In *Proceedings of IACSIT Hongcong Conference*, pages 144–149, 2012.
2. D Sheela, Naveen Kumar C and G Mahadevan. A Non Cryptographic Method of Sink Hole Attack Detection in Wireless Sensor Networks, In *Proceedings of International Conference on Recent Trends in Information Technology, ICRTIT*, pages 527–532, 2011.
3. D Mansouri, L Mokdad, Jalel Ben-othman and M Ioualalen. Detecting DoS Attacks in WSN based on Clustering Technique, In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2215–2219, 2013.
4. Jin Qi, Tang Hong, Kuang Xiaohui and Liu Qiang. Detection and Defence of Sinkhole Attack in Wireless Sensor Network , In *Proceedings of IEEE 14th International conference on Communication Technology (ICCT)*, pages 809–813, 2012.
5. *http* : *//www.isi.edu/nsnam/ns*.
6. Yanli Yu, Keqiu Li, Wanlei Zhoui and Ping Li. Trust Mechanisms in Wireless Sensor Networks: Attacks Analysis and Countermeasures, *Journal of Network and Computer Applications*, pages 867–880, 2012.
7. W Heinzelman, A Chandrakasan and H Balakrishnan. An Application Specific Protocol Architecture for Wireless Microsensor Networks, *IEEE Transaction on Wireless Communications*, 1(4):660–670, 2002.

8. Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, Wai-Choong Wong. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks, In *IEEE Communications Surveys and Tutorials*, 15(3):1223–1237, 2013.
9. Fenye Bao ,Ing-ray Chen, Moonjeong Chang and Jin-hee Cho. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-based Routing and Intrusion Detection, In *Proceedings of ACM Symposium on Applied Computing*, pages 1732–1738, 2011.

Geetha V obtained her Bachelor of Engineering degree from Mangalore university in 1999. She has obtained her MTech Degree in Computer Science and Engineering from VTU, Belgaum in 2004 by securing 2^{nd} rank. Currently she is pursuing her Ph.D in Department of Computer Science Engineering, National Institute of Technology Karnatka, Surathkal (NITK). She is also working as Assistant Professor in the Department of Information Technology, NITK, Surathkal since from year 2008. Her area of interest is Computer Architecture and Wireless Sensor Networks. She has published total 15 papers in international journals and conferences.

K Chandrasekaran is currently Professor in the Department of Computer Science and Engineering, National Institute of Technology Karnataka, having 26 years of experience. He has more than 120 research papers published by various reputed International journals, conferences which include IEEE, ACM, Springer *etc.*,. He has received best paper awards and best teacher awards. He serves as a member of various reputed societies including IEEE (Senior member), ACM (Senior Member), CSI, ISTE and Association of British Scholars (ABS). He is also a member in IEEE Computer Societys Cloud Computing STC (Special Technical Community). His areas of interest include Computer Networks, Distributed Computing (includes Cloud Computing and Security) and Business Computing and Information Systems Management.