ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (48-51), Month: October 2015 – March 2016, Available at: www.paperpublications.org

Dynamic Trust Management of Unattended Wireless Sensor Networks for Cost Aware Routing

Suja K.U

M.G University, Kottayam, Kerala, India

Abstract: **Unattended Wireless Sensor Networks (UWSNs) are characterized by long periods of disconnected operation and fixed or irregular intervals between sink visits. The absence of an online trusted third party implies that existing WSN trust management schemes are not applicable to UWSNs. In this paper, a trust management scheme for UWSNs to provide dynamic trust management is proposed. For trust data storage, geographic hash table is employed, it also helps to identify storage nodes and to significantly decrease storage cost. In order to mitigate trust fluctuations caused by environmental factors a subjective logic based consensus techniques is used. In this paper a set of trust similarity functions are exploited to detect trust outliers.**

Keywords: **Unattended Wireless Sensor Networks (UWSNs), GHT, GPSR, Subjective Logic.**

I. INTRODUCTION

The area of Wireless Sensor Networks (WSNs) has become popular in both the research community and industries. Wireless Sensor Networks usually consists of a large number of different types of sensor nodes that can monitor a wide variety of ambient conditions such as temperature, humidity, vehicular movement, pressure, etc. These sensor nodes can be easily deployed at a low cost for military and homeland security applications such as battlefield surveillance, as well as for civilian areas such as environment monitoring, E-health, and industrial automation, here a trusted third party is present to collect the data in a near to real time fashion . Although many WSNs operate in such a mode, there are WSN applications that do not fit into the real time data collection model. The lack of regular access routes and the size of the surveillance area would require a mobile sink to collect data periodically i.e. Unattended WSNs (UWSNs) with a mobile sink visiting the network at either fixed or irregular intervals to collect data. Trust Supervision becomes very important for detecting malicious nodes in unattended hostile environments. An efficient trust management scheme can handle trust related information in a secure and reliable way, also secure routing of data, secure distribution of data and trusted key exchange can be established. Here a trust management scheme is proposed for collecting data from unattended nodes and also for efficient trust generation as well as robust trust data storage in UWSNs. A central issue for trust Supervision in UWSNs is how to store trust data without relying on a trusted third party. Initially, few simple trust Supervision schemes are considered as a first-step attempt to address the existing trust problems in UWSNs i.e. Trust Data Local Storage Scheme, Trust Data Distributed Storage Scheme and Advanced Scheme. After analyzing the shortcomings of these simple schemes, an Enhanced Advanced Scheme is proposed based on a Geographic Hash Table (GHT), Grid Partitioning and Similarity measure of interaction. Dynamic trust management of UWSN's helps to overcome the drawbacks of three proposed schemes i.e. Trust data local storage, Distributed trust data storage and advanced scheme.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (48-51), Month: October 2015 – March 2016, Available at: www.paperpublications.org

II. RELATED WORK

Several solutions have been recently proposed for trust Supervision in WSNs. In [1] Reputation-Based Framework for High Integrity Sensor Networks (RFSN) is proposed. This method records the interaction between nodes and revises the current trust evaluation through direct and indirect reputation, so the trust value of nodes is objective and true. In [2] Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks (GMTS) is proposed. This method uses distributed trust management within the cluster and centralized trust management across clusters, so that it could reduce interaction costs between nodes. Since the GMTS does not focus on trust evaluation of a single node, it requires less memory to store the trust records compared with other trust evaluation models. In [3] a trust model based on grid (GBTM) is proposed. It is similar to the trust model based on cluster and each grid has a cluster head, then the trust value of nodes are independently calculated layer by layer. Besides, [4–6] proposed trust evaluation of WSNs based on cluster, in which the cluster members layer and the cluster heads layer use different methods to calculate trust values; [7, 8] evaluate the trust value of nodes through aggregating direct and indirect trust. These methods have done adequate research on the accuracy of evaluating the trust value of nodes, while they also have consumed too much energy of sensor nodes. Most of the trust Supervision solutions developed for traditional WSNs, however, rely on the presence of an online trusted third party, e.g., to store and distribute trust data. They cannot be applied directly to UWSNs due to the absence of the sink (or the base station). In paper [16], in order to save energy of sensor nodes, the WSNs is divided into several grids, and the trust value of grids is calculated rather than evaluating the trust value of nodes .They evaluated the similarity measure of trust between nodes within grid to detect malicious nodes. Besides [17] proposes three trust management schemes for UWSNs i.e. Trust Data Local Storage Scheme, Trust Data Distributed Storage Scheme and Advanced Scheme. This paper proposes a trust management scheme, Enhanced advanced scheme based on GHT, GPSR(GPSR can use local topology information to find correct new routes quickly) and on similarity measure theory and introduce a method to collect data from unattended nodes in unattended areas . It divides WSNs into several grids, and uses similarity measure theory of fuzzy which has been widely used in many areas such as image registration [9], information retrieval [10] and multimedia technologies [11], etc.

III. DYNAMIC TRUST MANAGEMENT OF UWSNS

In traditional WSNs, a trusted third party, e.g., base station, is always present to keep and calculate received trust opinions. The queries of sensors' trustworthiness are also sent to and answered by the base station. However, since UWSNs do not have a base station, trust opinions of sensors need to be stored in sensors instead. Therefore, once sensor bi generates an opinion Tj, ti at time interval t, it either stores Tj, ti locally or sends Tj, ti i to other nodes. Next three trust data storage schemes is considered. Then an enhanced advanced scheme is proposed to improve the basic schemes. First scheme is Trust data local storage, in this scheme trust producer and trust manager are same i.e. in this scheme trust opinion is generated and stored within the same node. The main drawback of Trust data local scheme is that adversary can easily identify trust manager node as trust producer and trust manager are same .Second scheme is Trust data distributed storage, in this scheme each node is assigned with 'n' randomly selected trust managers which are not the direct neighbor nodes so that it is difficult for the adversary to identify the trust manager node within the network. Third scheme proposed is Advanced scheme, this is an efficient scheme that employs GHT where nodes can put and get data based on their data type, i.e., Put (Data Type, Data Value) and Get (Data Type). Since a sensor ID is unique in the network, trust producers are able to put trust opinions to trust managers based on the ID, i.e., Put (sj, Tj, ti). Trust consumers are able to get trustworthiness from trust managers using the same sensor ID, i.e., Get (sj). In other words, trust opinions are pushed by, and stored at the same trust manager node. Meanwhile it enables trust consumers to pull trustworthiness from the trust manager nodes consistently. Neither trust producers nor trust consumers need to store the IDs of trust manager nodes, reducing storage cost significantly.

The proposed scheme is an enhancement of advanced scheme. In advanced scheme the trust information regarding all involved sensors within the network is to be calculated individually, this causes large energy loss and time consumption. So in order to overcome this drawback grid partitioning is employed in the network. In grid partitioning the WSN is divided into several grids. Sensor nodes are randomly deployed in a square monitoring area with the side length L. The whole monitoring area is divided into several square grids with the side length Rc,and each grid has an unique ID .The base station is located in the center. unattended nodes is assumed to be located at corners of monitoring area which is at

largest distance from base station. Then the energy consumption can be reduced by calculating the trust value of grids rather than calculating the trust value of nodes. At the end of each period, every grid evaluates the similarity measure of interaction between its neighboring grids to determine the presence of malicious nodes within the neighboring grids. [16] proposed a node trust evaluation method, which only count the failed number of co-operations between grids, because the nodes number in each grid is different so the average failed number of co-operations between grids is used this method is employed here .By using Min Average Theory the similarity measure of interaction between two neighbor grids can be calculated .The mismatch in similarity measure of interaction shows the presence of malicious node in that particular grid. After analyzing the similarity measure of interaction between grids, the similarity measure of trust of all nodes within the grid is evaluated. Thus we can identify the malicious node, and the detected malicious node is excluded from the network. A node is said to be malicious if it captured by the enemy at any point and start passing erroneous information or drop packets. A node is more likely to become malicious if it has low energy or if it is surrounded by malicious nodes. After excluding malicious nodes within the network, efficient path with least hop count is found by GHT and GPSR routing.

Steps employed to attain trust management in UWSN's;

1. Consider the nodes.
2. Select the relay nodes.
3. With the help of relay nodes tracking of unattended nodes is done.
4. Constantly monitor the information of moving nodes.
5. Using on demand protocol handover of information is done and assures the node is trustworthy.
6. Find multipath routes with intermediate delay method.
7. Choose the optimized path if relay nodes fail.
8. Self-rerouting is implied.
9. Add security features.

GHT hashes keys into geographic coordinates, and stores a key-value pair at the sensor node geographically nearest the hash of its key. The system replicates stored data locally to ensure persistence when nodes fail. A data object is associated with a key and each node in the system is responsible for storing a certain range of keys. A name-based routing algorithm allows any node in the system to locate the storage node for an arbitrary key. This enables nodes to put and get files based on their key, thereby supporting a hash-table-like interface GHT uses the GPSR geographic routing algorithm as the underlying routing system. Greedy Perimeter Stateless Routing, GPSR, uses geography to achieve small per-node routing state, small routing protocol message complexity, and extremely robust packet delivery on densely deployed wireless networks, under GPSR, packets are marked by their originator with their destinations' locations. As a result, a forwarding node can make a locally optimal, greedy choice in choosing a packet's next hop. Specifically, if a node knows its radio neighbors' positions, the locally optimal choice of next hop is the neighbor geographically closest to the packet's destination. Forwarding in this regime follows successively closer geographic hops, until the destination is reached. GPSR delivers the vast majority of packets in the optimal number of hops. GPSR's benefits all stem from geographic routing's use of only immediate-neighbor information in forwarding decisions. The data from unattended nodes are collected by neighboring nodes of the unattended nodes in the optimal path formed within the grid between sink and source.

IV. CONCLUSION

In Dynamic Trust Management of UWSN's For Cost Aware Routing, an efficient and robust trust management schemes for UWSNs is proposed. The enhanced advanced trust scheme facilitates high reliability of trust data compared with the less sophisticated approaches and can effectively improve nodes lifetime also. It takes the advantage of GHT, GPSR routing, Grid partitioning and Similarity theory to find storage nodes, to route trust data and to collect data from unattended nodes. In Dynamic Trust Management Of UWSN's For Cost Aware Routing , several methods are proposed to mitigate trust pollution attacks based on various trust similarity measures. The transmission range vs. network lifetime

graph shows that the enhanced scheme have more network lifetime compared to the advanced scheme and scheme I. Scheme I (Trust data local storage) have the worst performance compared to the other two schemes. Network lifetime is very less for scheme I than other two schemes, AS and EAS. Simulation results show that proposed scheme has much lower storage costs. Combining advanced trust scheme with grid partitioning and by similarity measure theory, data from unattended nodes is obtained.

REFERENCES

[1] Ganeriwal S, Balzano L K, Srivastava M, Reputation based frame-work for high integrity sensor networks, ACM Transactions on Sensor Networks 4(2008) 1-37.

[2] Shaikh R A, Jameel H, d'Auriol B J, et al, Group-based trust management scheme for clustered wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 20(2009) 16981712.

[3] Yan Binyu, Zhang Yongqi, Dong Minjian, A trust model based on grid for wireless sensor networks, Journal of Computational Information Systems 8(2012) 405-414.

[4] J. Zhang, R. Shankaran, M. A. Orgun, et al, A trust management architecture for hierarchical wireless sensor networks, in: Proc. IEEE 35th Conference on Local Computer Networks, 2010, pp. 264-267.

[5] J. Zhang, R. Shankaran, M. A. Orgun, et al, A Dynamic Trust Establishment and Management Framework for Wireless Sensor Networks, in: Proc. IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing, 2010, pp. 484-491.

[6] V. R. S. Dhulipala, N. Karthik, R. M. Chandrasekaran, A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks, Wireless personal communications 70(2013) 189-205.

[7] P. Trakadas, S. Maniatis, P. Karkazis, et al, A novel flexible trust management system for heterogeneous wireless sensor networks, in: Proc. International Symposium on Autonomous Decentralized Systems, 2009, pp. 1-6.

[8] T. Zahariadis, P. Trakadas, H. C. Leligou, et al, A novel trust-aware geographical routing scheme for wireless sensor networks, Wireless personal communications 69(2013) 805-826.

[9] F. C. Calnegru, Magnitude Type Preserving Similarity Measure for Complex Wavelet Based Image Registration, in: Proc. Advanced Concepts for Intelligent Vision Systems, 2013, pp. 102-113

[10] Gupta Y, Saxena A K, Saini A, et al, Development of hybrid similarity measure using fuzzy logic for performance improvement of information retrieval system, in: Proc. Computing for Sustainable Global Development, 2014, pp.1-5.

[11] U R Rehman Z, Hussain F K, Hussain O K, Frequency-based similarity measure for multimedia recommender systems, Multimedia systems 19(2013) 95-102.

[12] Zhang Jinxue, Zhang Ming, Energy efficient least spanning routing tree algorithm based on virtual grid in wireless sensor networks, Sensors and Transducers 158(2013) 113-119.

[13] Kim K, Bang H, Jin S, Efficient data collection for smart grid using wireless sensor networks, in: Proc. Consumer Electronics (GCCE), 2013 IEEE 2nd Global Conference on. IEEE, 2013, pp. 231-232.

[14] Tang G, Xie Y, Tang D, et al, An Adaptive Grid Division algorithm for target location in wireless sensor networks, in: Proc. Conference Anthology, IEEE. IEEE, 2013, pp. 1-6.

[15] Ishmanov F, Kim S W, A secure trust establishment in wireless sensor networks, in: Proc. Electrical Engineering and Informatics (ICEEI), 2011 International Conference on. IEEE, 2011, pp. 1-6.

[16] A Grid Trust Evaluation Method for Wireless Sensor Networks based on Similarity Measure Theory⋆ Haibo SHEN∗, Kechen ZHUANG, Hong ZHANG, Journal of Computational Information Systems 11: 8 (2015)

[17] A Trust Supervision in Unattended WSN using Novel Approaches G.Bakkiyaraj1, R.Shanthipriya2, IJISET – International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 2, February 2015.