Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 83 (2015) 33165-33167

ISSN: 2229-712X

A Survey on Trust Systems for Clustered Wireless Sensor Networks

Pranav Avinash Marathe, Karthik B Iyer, Saddam Shaikh and Sharmila A Chopade

DY Patil Institute of Engineering and Technology, Pune, India.

ARTICLE INFO

Article history:

Received: 16 January 2015;

Received in revised form:

3 June 2015;

Accepted: 13 June 2015;

Keywords

LGTS,

Wireless Sensor Networks,

Trust system.

ABSTRACT

There are many primitive trust systems which have adopted unique approach for communication in Wireless Sensor Networks. These traditional trust systems do not meet the requirements like maintaining resource efficiency and dependability between nodes in Clustered Wireless Sensor Networks. This is because of their high overhead and low dependability. LDTS (Light-weight and dependable trust system) proposes low communication overhead and makes efficient use of energy resources by proposing light-weight algorithm. Also LDTS (Light-weight and Dependable Trust System) proposes dependable trust system that helps improving system efficiency by reducing effect of malicious nodes. As compared to traditional trust systems LDTS (Light-Weight and Dependable Trust System) demands less memory .So it can be said that LDTS is light weight and dependable trust system for communication in clustered wireless sensor networks.

Introduction

Wireless sensor networks consist of large number of sensor nodes. The sensor nodes are able to process the data and transfer the information to the user. A sensing node transceiver, sensor and a power supply sub system. The transceiver is used for communication between neighboring nodes. Sensor is used for sensing the data and power supply subsystem provides power to the node. Each node in Wireless Sensor networks communicates by using multi-hop strategy and they act as router as well as a host. In WSN (Wireless Sensor Networks) there are thousands of sensor nodes deployed. Wireless Sensor networks have functional ability to monitor the events, collect and process data and send it to the end users. For communication in Wireless Sensor networks the sensor nodes are grouped together to form a cluster .This method is called as Clustering. Adopting Clustering in Wireless Sensor Networks helps to maintain scalability. Clustering thus helps to monitor the processing of data efficiently and also provides proper routing path to transmit information to the interested users. Each node has a trust value based on which the reputation of a particular node can be determined. Trust plays a key role in adding or deleting a particular node in the wireless sensor network. The creation of nodes and the operations carried on the nodes depends on the trust values. The trust is nothing but a quantitative value through which the reputation of a particular node is determined. Establishing trust between the nodes of wireless sensor networks helps the network to secure the data that is being passed to the respective node. There are many primitive trust systems like GTMS[8],HTMP[9],HTRM[11],ATRM[12],TCHEM[10] which have adopted the concept of trust for communication in WSN(Wireless Sensor Networks.)

Motivation

Dependability between nodes and resource efficiency must be prioritized first while considering a wireless sensor network. But the existing traditional trust systems neglect these priorities which results in low dependability and high overhead. Limited work has focused on the efficiency of resources when using clustered wireless sensor network. The priorities while designing a trust system for any WSN that it must lightweight to serve and resolve as many nodes as it needs. Based on the requirements of WSN to design dependable trust system some traditional algorithms are developed. But most of these algorithms fail to consider the resource efficiency or some the algorithm are very complex that it cannot be evaluated on a cluster member on node level. LDTS(Light weight and Dependable trust system)helps to resolve these problems by providing light weight algorithm and also maintains dependability between the nodes.

Related work

Research regarding Trust system has always been the point of attraction for scholars. Any strategies and algorithms have proposed such systems for wsn's. But these system or strategies suffer in many perspectives such as to meet the resource constraint environment when considering a wireless sensor network especially multilevel or large scale. But they do not meet the terms which required for designing a trust system like resource efficiency and dependability.

1. GTMS[8],a Group-Based Trust Management Scheme for clustered WSNs. GTMS focuses on trust values of a group of nodes i.e. clustered nodes rather than focusing on finding trust value of individual node. This approach gives wsn's about possessing less memory to store trust records at each node. GTMS helps in decreasing the evaluation cost associated of the trust evaluation of distant nodes. But GTMS uses broadcast based strategy to collect feedback from the CM's of a cluster, which results in requiring significant amount of resources and power.
2. HTMP [9], Based on the two aspects of trustworthiness i.e. social trust and QoS (quality of service) trust, a hierarchical dynamic trust management protocol for cluster-based WSNs is proposed. Using unique technique used in petri-net which is also called as stochastic petri-net the authors developed a probability model to analyze protocol performance and then by obtaining a ratio of subjective trust and objective trust based on the ground truth node status. However implementing such complex system at each node or CM level is unrealistic.
3. TCHEM [10], a Trust-Based Cluster Head Election Mechanism has been proposed.

Tele:

E-mail addresses: pheonixrad@gmail.com

SR NO	PAPER	CONFEREN-CE	APPROA-CH
1	"Group-based trust management scheme for clustered wireless sensor networks,"	IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp.1698–1712, Nov. 2009.	This System uses Broad cast Based technology to take feedback from every node which results in high consumptions of resources and power.
2	"A framework for trust-based cluster head election in wireless sensor networks,"	Proc. Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22	This trust system gives each node a unique id and these unique id's are used to select a cluster head. It will prevent malicious nodes from getting elected as cluster heads
3	"Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,	IEEE Trans. Netw. Service Manag., vol. 9,no. 2, pp. 169–183, Jun. 2012.	It uses two kinds of trust values to be computed at each node but HTMP is very unrealistic because of its assumption.
4	"Trust-based security for wireless ad hoc and sensor networks,"	Computer Commun. vol. 30, pp. 2413–2427, Sep. 2007.	This approach induces a mobile agents running at each nodes so that whenever the requested the node are capable of providing their own reputation.
5	"Behavior Based Trust Management"	International Journal of Computer Trends and Technology- volume3Issue2- 2012	This technology detects the malicious nodes and separates them from neighboring nodes.
6	"Hybrid Trust and Reputation Management"	Springer Science Business Media, LLC 2009	For the distributed applications this technique is used. This shows the effective results to manage the relationship between nodes and the clusters.

This strategy is designed for cluster based network model in which some nodes have unique local ID's.This algorithm restricts the faulty or malicious nodes from being elected as CH. This algorithm prevents the sharing of information between sensor nodes in a network. Thus this technique reduces the effect of bad mouthing attack. But the drawback of this system is it does not cover trust system in detail which results in numerous key issues of trust management.

4. ATRM [12], Trust Based approach for Wireless Sensor Network Using Agent for Each Cluster, this strategy is designed for calculating trust values of neighboring nodes with the help of the agent. The agent is responsible for computing the trust and reputation of the distant nodes with the help of various formulas. The trust value calculated depends on the amount of the packet data sent between the nodes. As it uses agent for computing the trust values for each node there is significant usage of resources also. This is the drawback of this strategy.

5. BBTM [13], Behavior Based Trust Management is used to detect the malicious nodes makes them separated from the neighboring nodes. This strategy focuses on the behavior of the nodes by computing the geometric mean and QoS i.e. Quality of Services characteristics of the node .Because of this only trusted nodes can participate in the routing messages. This Strategy makes the routing path secure by detecting the misbehavior of the node.

6. HTRM [11], Hybrid Trust and Reputation Management does not tend to include metrics and the methods for finding and combining of the hard and soft trust. Hybrid Trust and Reputation Management ensures security in the distributed applications. This strategy show effective results to manage the relationship between the nodes and clusters.

Acknowledgement-

We are grateful to our teacher guide and project coordinator for the guidance they gave us in preparing this paper successfully .We would also like to express gratitude towards the excellence of college and towards friends and family for their aid and support.

Future Work

With many advantages over traditional trust systems, LDTS justifies to be dependable trust system. The detection of malicious nodes can be taken into consideration and can be deleted so as to avoid Collapse of WSN network. Also an intruder can interpret on sending data and affect the system performance so such data sending can be encrypted to make it secure and safe. This implies an important future work for wireless sensor network.

References

[1] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, Oct. 2002.

[2] D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," Comput. Commun., vol. 32, no. 4, pp. 662–667, Apr. 2009.

[3] Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energy-efficient clustering solution for wireless sensor networks," IEEE Trans.Wireless Commun., vol. 10, no. 11, pp. 3973–3983, Nov. 2011.

[4] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, Oct. 2004.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Netw., vol. 4, no. 3, pp. 1–37, May 2008.

[6] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," IEEE Commun.Mag., vol. 46, no.2, pp. 112–119, Feb. 2009.

[7] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proc. IEEE, vol. 98, no. 10, pp. 1752–1754, Oct. 2010.

[8] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[9] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9, no. 2, pp. 169–183, Jun. 2012.

[10] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in Proc. Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

[11] Efthimia Aivaloglou, Stefanos Gritzalis "Hybrid trust and reputation management for sensor networks" Springer Science Business Media, LLC 2009

[12] Yenumula B. Reddy "Trust based approach in wireless sensor networks using and agent to each cluster" Department of Computer science, Grambling State University, Grambling, LA 71245, USA.

[13] Ch.Satya Keerthi.N.V.L, A.Manogna, Ch.Yasaswini, A.Aparna, S.Ravi Teja "Behaviour based Trust Management using geometric mean approach for Wireless Sensor Networks" International Journal of Computer Trends and Technology- volume3 Issue2- 2012.