Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Energy Efficiency through Trust System Watchdog Optimization for WSN

Valabhoju Laxmi Prasanna
M.Tech,
Department of Computer Science and Engineering,
Christu Jyothi Institute of Technology & Science.

J.Purna Prakash
Assistant Professor,
Department of Computer Science and Engineering,
Christu Jyothi Institute of Technology & Science.

Abstract:

Many believe that the technical surveillance systems, wireless sensor networks (WSN) are designed to protect is critical. Unfortunately, this type of technology is energy-intensive and thus substantially limit the duration of the WSN. Although the initial studies on the different solutions proposed for WSNs and realized the importance of the effectiveness of the system has to be reliable, the watchdog technology, which can be among the best units to optimize the energy consumption is neglected. In this article, we have confidence in the current system inefficient use of technical surveillance shows, and then to use Sentinel to reduce energy costs to offer a range of optimization methods, while at the maintaining the appropriate level of system security. Our theoretical analysis and practical algorithms to contribute effectively and efficiently to the reliability of the sensor nodes and destination nodes according to their plan that will consist of supervisory duties.We are on top of a platform WSNET simulations to evaluate and test our algorithms through experiments in our laboratory is supported by WSN. The results confirmed that our monitoring optimization techniques successfully (in terms of accuracy and robustness of the trust <0.06) without sacrificing security of energy could save at least 39.44%, in some cases, increases security against some attacks.

Index Terms:

Wireless network, secure, energy efficiency, security of technical surveillance sensors.

INTRODUCTION:

Traditional security mechanisms (for example, encryption methods, authentication and logical access control, etc.) required to complement, belief systems are widely used in wireless sensor networks (WSN for short) is used to protect the nodes will be attacked by “legitimate” sensors (nodes that are compromised or selfish or failure). These nodes identified “legitimate” can bypass traditional security defenses, but alternatively or bad your bad reputation because of past conduct reliable system can be captured. In other words, faith is based on the reputation of the sensor node and the previous behavior, and integrity and internal nodes can be used to model the states. Although many safety recommendations trustees global network system (ie, indirect trust) with a view to the field of trust (ie direct counting) to extend the permit, always ensure that the experience of past behavior is based in recommendations. In short, based sensor nodes past behavior (for short of WSNTSs) is the basis for building trust WSN system.However, the business traffic between the WSN confidence to build a reliable system for the collection of past behavior is not a trivial task. In the first place, powerful base station (when WSN is a flat topology) and cluster headaches (as a hierarchical topology), which is likely to both business needs to communicate with the network (or the entire cluster) all sensor nodes (node distances are) who do not have the ability to experience the remote nodes (eg sector) can not get into the communication range.

Secondly, some sensor nodes to their neighboring nodes, or to communicate with their business relationship business requirements may not occur at very low frequency. Lazy trade traffic with the previous behavior of these nodes are difficult to collect. Third, since the behavior of a type of confidence that this is a conscious experience of the context and type cannot be used to build confidence. For example, a well-routing packet transmission node’s behavior in the past does not mean that reliable survey data reported to the node (for example, multi hope routing that can be drawn from the conduct of faith in the sense data is). Therefore, all kinds of confidence for WSN to a wide range of business traffic can remember. To meet these challenges and to facilitate the collection of past behavior, the current WSNTSs technology adopted a so-called watchdog.

Dedicated as a predefined frequency for dynamic and reliable activities to interact directly with their neighborhood nodes to begin to use this technology, sensor nodes can run monitoring. They can get first hand experience of the behavior of these nodes, even if there are commercial activities. For example, a node within a certain period of time actively sensing data can query other nodes (even if in reality it does not require these data for commercial reasons)While a very effective method for monitoring technology to build the foundation of WSNTS as has been proved, the struggle, the energy efficient design of WSN theory introduces a large amount of additional energy consumption. Charging or replacement of the power of these nodes is very difficult and expensive. Because of these problems, saving energy plays a very important role in the design of modern WSN.

However, to our knowledge, no current WSNTSs enough to save the energy consumed by a technical monitoring solutions (for example, the use of energy watchdog faith conflict has not been inspired by the previously discussed) offer. how often allow for appropriate monitoring. The next dog unnecessary operation of this type of methods of flood detention and without causing much additional safety benefits could waste a lot of energy. Therefore, to save energy and to assess the confidence enough to collect past behavior, an intelligent scheduler is very important watchdog.we WSNTSs monitoring technology to optimize (in terms of accuracy and robustness of the trust) to balance efficiency and energy security will fill this gap. Our ultimate goal, driven by the control functions to reduce energy costs to the extent possible, the confidence and strength to a sufficient level to maintain the purity of.

To achieve this goal, we have two techniques for monitoring the level of optimization. These nodes have to deal with more than one partner and is expected to start the attack. We optimal tracking position (given a destination node) Overall risk (in terms of energy consumption and security) are looking to minimize. Secondly, we optimize the frequency control and reduce redundancy. Specially,(Eg, trusted or untrusted) may require less monitoring of activities (ie, low-frequency guard dog) to deepen the sensor node whose behaviors are more uncertain than nodes with higher reliability determined. So we trusted destination nodes according to appropriate monitoring frequency. In short, we are making significant contributions to this document three.

We WSNTSs inefficient use of existing techniques in monitoring conflict-induced confidence novel energy are conducting a study to appear. The conflict fully addressed in the literature, previous research has not. WSNET platform for our test lab in collaboration brings income. The experimental results have confirmed the effectiveness of our design successfully.

SYSTEM PRELIMINARIES:

We have four high-level model using WSN and formalize WSNTS. Specifically, the first thing we have a model system for describing WSN. We then model the law of WSN energy consumption. Then we have a threat model and a trust model, respectively WSNTS think about. For ease of reference, in this article we summarize the key used notation.

System Model:

We have an undirected graph G = (V, E), where E j V represents a sensor node WSN and EI as a WSN nodes and VJ model means that you are in a range of communication (ie in , District). We consider how to design a WSN topology flat, although our solutions work in the field, and such other topologies such as clustering WSN adapt. In both cases, the spatial distance between the sixth and VJ and Ri j is the scope of communication. Consider EI J ≤ ≤ Ri E WSN and GJ J and R J is an example of the IFF system models. As we define the neighborhood nodes bilateral V. We Bi = {v J | JJ EI E} = {v | } J and J ≤ ≤ JR laughed. Figure 1 shows an example of our model WSN system.

As we can see, even in v3 and v4 v2 communication range (ie, D23 and D24 ≤ ≤ R2 R2), E23 and E24 do not exist (for example, V3, V4 / B2) because D23> D24 and R3> R4. Up a supervisory law to formalize, with constant time intervals of equal size in a sequence of time intervals are separated by space. I J W we define as working node will monitor time interval T VJ monitor its neighboring node is executed. By weight of a working monitor sentinel node and the destination node Jammu you a two-way communication between VJ occur. In other words, you have a request response packet VJ wait for VS Jay would send. The requirement to monitor the work of the monitoring and only if I can assume w j jj ≤ ≤ Ri and RJ (ie it exists in El G J) VJ. In other words, the node can act as a watchdog.

RELATED WORK:

We have state-of-the-art literature WSNTSs, especially systems designed to manage real confidence WSN come again. In practice, the trust system design and general security (identity and alienation, “legitimate” sensor nodes are compromised by malicious or selfish refuse to help others, or for the purpose of failure due to configuration errors and bugs WSN are distributed), and it can include protecting the functionality of WSN. In the literature, WSNTS usually unreliable and corrupt data sensing is applied to prevent, protect or fixed multi-hop routing or both. Many of these people say WSNTSs a watchdog or a monitoring technology for the collection of the trust behavior, adopt and monitor the data to detect and get a good performance in multi-hop routing. Past behavior they believe they can accumulate enough to assess watchdogs this realization.

For example, the nodes for data collection techniques employed for active surveillance, and compromised by faulty nodes or report invalid data to detect an outlier detection algorithm is applied. It works as a sensor node identification disobedient sensor nodes have a guard dog, as the routing behavior in their vicinity and listen for these nodes being used to prevent future path enables.However WSNTSs can greatly improve the efficiency and security of WSN, the total cost of energy, driven by the construction of these systems cannot be ignored. Jokes, WSNs are generally for a long period of time are required to operate in an automatic mode (for example, two or three years without charge batteries), they generally have limited resources and are equipped with batteries.

For this reason, the WSN can limit significantly longer life expectancy for the trust management costs is huge. State-of-the-art in the search for individual WSNTSs realize the importance of the issue of the effectiveness and the initial solution proposed in their design. In particular, to identify the trustees (because of less use of storage can save energy) from a geographic hash table putting faith offer an efficient storage model, helping all the sensor nodes estimated energy cost of implementing an energy observer neighboring nodes for each packet transmission, and then as the next hop on the way to allow the selection of the most efficient node.In addition, clustering technology is widely used in the literature for WSN WSNTSs and high energy efficiency.

From the base station sensor node (cluster members) for the management of a select number of cluster head, power consumption can be reduced due to less communication distance. Based on the cluster topology (ie the trust recommended) between members of the cluster and / or cancellation through the reaction between the cluster head reduces energy, and therefore proposed a WSNTS lighter. Despite these early efforts, a watchdog techniques, perhaps the most important WSNTS unit energy consumption is taken into consideration. We are planning to optimize sentinel in this document are conducting a new study. Our research literature is very different from the energy efficient and opens a new door to designing WSNTS.

First, instead of the memory used to save power to the contrary, our research takes as the central theme of conservation of energy and optimize the technique for the first time Sentinel. Second, although it is safe, efficient and reliable way to efficient routing algorithm to select the next hop node provides the energy used to produce it WSNTS which is the main problem we have to solve today’s documents You cannot reduce. Third, clustering technology, which is a hierarchical architecture topology for WSN save energy by restructuring the opposite, our research will save energy by reducing redundant WSNTS foundation trust.

Even better, our solutions can be applied to clusters WSNs is to further reduce the cost of energy. Finally, but most important, energy-efficient design to reduce unnecessary communication WSNTS recommendations (both used) is called faith. In contrast, our research to save power by reducing unnecessary monitoring goes a step further (also called first experience). First-hand experience is the more expensive second-hand (in terms of energy consumption) is. The energy saving results in a more advanced opportunities.

CONCLUSION:

We take the first step to answer a question, the important WSNTS research still maintain adequate security when the trust (ie, first-hand experience) of the basic foundations are reduced. The problem for the theoretical analysis and extensive experiments take a very positive result. Our study follows the process of collection of first-hand experience by optimizing the design of energy-efficient lighting WSNTS a promising research direction.

REFERENCES:

[1] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensornetworks,” Commun.ACM, vol. 47, no. 6, pp. 53–57, 2004.

[2] M. L. Das, “Two-factor user authentication in wireless sensor networks,”IEEE Trans. Wireless Commun., vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[3] Y. Zhou, Y. Zhang, and Y. Fang, “Access control in wireless sensornetworks,” Ad Hoc Netw., vol. 5, no. 1, pp. 3–13, 2007.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routingmisbehavior in mobile ad hoc networks,” in Proc. 6th Annu.Int. Conf.Mobile Comput.Netw., 2000, pp. 255–265.

[5] E. Shi and A. Perrig, “Designing secure sensor networks,” IEEE WirelessCommun., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-basedframework for high integrity sensor networks,” ACM Trans. SensorNetw., vol. 4, no. 3, 2008, Art. ID 15.

[7] R. A. Shaikh, H. Jameel, B. J. d’Auriol, H. Lee, S. Lee, andY.-J. Song, “Group-based trust management scheme for clustered wirelesssensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11,pp. 1698–1712, Nov. 2009.

[8] G. Zhan, W. Shi, and J. Deng, “Design and implementation of TARF:A trust-aware routing framework for WSNs,” IEEE Trans. DependableSecure Comput., vol. 9, no. 2, pp. 184–197, Mar./Apr. 2012.

[9] S. Zheng and J. S. Baras, “Trust-assisted anomaly detection and localizationin wireless sensor networks,” in Proc. 8th Annu. IEEE Commun.Soc. Conf. Sensor, Mesh, Ad Hoc Commun.,Netw. (SECON), Jun. 2011,pp. 386–394.

[10] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, “A novelapproach to trust management in unattended wireless sensor networks,”IEEE Trans. Mobile Comput., vol. 13, no. 7, pp. 1409–1423, Jul. 2014.

[11] X. Li, F. Zhou, and J. Du, “LDTS: A lightweight and dependabletrust system for clustered wireless sensor networks,” IEEE Trans. Inf.Forensics Security, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[12] D. Wang, T. Muller, Y. Liu, and J. Zhang, “Towards robust and effectivetrust management for security: A survey,” in Proc. 13th IEEE Int. Conf.Trust, Secur., Privacy Comput. Commun.(TrustCom), 2014.

[13] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, “A survey of trustand reputation management systems in wireless communications,” Proc.IEEE, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

[14] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, “Trust managementsystems for wireless sensor networks: Best practices,” Comput.Commun., vol. 33, no. 9, pp. 1086–1093, 2010.

[15] F. G. Nakamura, F. P. Quintão, G. C. Menezes, and G. R. Mateus,“An optimal node scheduling for flat wireless sensor networks,” in Proc.4th Int. Conf. Netw., 2005, pp. 475–482.

[16] A. Salhieh, J. Weinmann, M. Kochhal, and L. Schwiebert, “Powerefficient topologies for wireless sensor networks,” in Proc. Int. Conf.Parallel Process., Sep. 2001, pp. 156–163.

[17] J.-H. Cho, A. Swami, and R. Chen, “A survey on trust management formobile ad hoc networks,” IEEE Commun. Surv.Tuts., vol. 13, no. 4,pp. 562–583, Oct./Dec. 2011.

[18] Y. Yu, K. Li, W. Zhou, and P. Li, “Trust mechanisms in wireless sensornetworks: Attack analysis and countermeasures,” J. Netw. Comput.Appl.,vol. 35, no. 3, pp. 867–880, 2012.

[19] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor network security:A survey,” IEEE Commun. Surv.Tuts., vol. 11, no. 2, pp. 52–73,Apr./Jun. 2009.

[20] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, “Locationcentricisolation of misbehavior and trust routing in energy-constrainedsensor networks,” in Proc. IEEE Int. Conf. Perform., Comput., Commun.,2004, pp. 463–469.