INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 6 (2017) PAGES 2452 - 2456
RECEIVED : 25.10.2017 PUBLISHED : 13.11.2017
Nov 13, 2017

Wireless Sensor Networks using Active Trust SCHEME DESIGN

[1]A.Kalaivani, [2]Dr.P.Rajaram,

[1]PG Scholar, Department Of Computer Science And Engineering, Maha Barathi Engineering College, Chinna Salem, Villupuram,

[2]Supervisor And Assistant Professor, Dept Of Computer Science And Engineering, Maha Barathi Engineering College, Chinna Salem, Villupuram.

Abstract:

Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. To conquer that challenge, an active detection-based security and trust routing scheme named Active Trust is proposed for WSNs. The most important innovation of Active Trust is that it avoids black holes through the active creation of several detection routes to quickly detect and obtain nodal trust and thus improve the data route security. More importantly, the generation and distribution of detection routes are given in the Active Trust scheme, which can fully use the energy in non-hotspots to create as many detection routes as needed to achieve the desired security and energy efficiency. Both comprehensive theoretical analysis and experimental results indicate that the performance of the Active Trust scheme is better than that of previous studies.

Keywords: WSN, Detection, Hotspot.

1. INTRODUCTION

In many Wireless Sensor Network (WSN) applications, sensors are spatially distributed in a finite area so as to monitor physical or environmental conditions, such as pressure, humidity, temperature, etc. and also to transmit the sensed data to a base station cooperatively. In addition, at times, a set of target points has to be monitored in a given area. On the one hand, to provide a deterministic quality of service guarantees, every point of interest should be monitored by at least one sensor at all times. On the other hand, the energy consumption of sensors should be minimized since in most cases sensors are battery powered. Therefore sensors should have their power supplies turned off when they are not in use top reserve energy. Due to this limitation, a critical issue becomes how to prolong the lifetime of WSNs while also assuring the service quality of coverage. Thus, research on energy efficient sensor coverage problem has been extensively investigated in the literature. For a typical target coverage problem in WSNs, the network lifetime is defined as the time duration that all the target points are monitored. As pointed out in, network lifetime can be prolonged by alternating the working modes of sensors between settings of “on” and “off”. In other words, schedule the entire time duration into a number of rounds and only turn-on the power supplies of a subset of sensors to monitor the target points in each round. Supposing that, all the sensors can work two time units, then by alternating the “on” and “off” modes, we can monitor all the target points for three time units. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 6 (2017) PAGES 2452 - 2456
RECEIVED : 25.10.2017 PUBLISHED : 13.11.2017
Nov 13, 2017

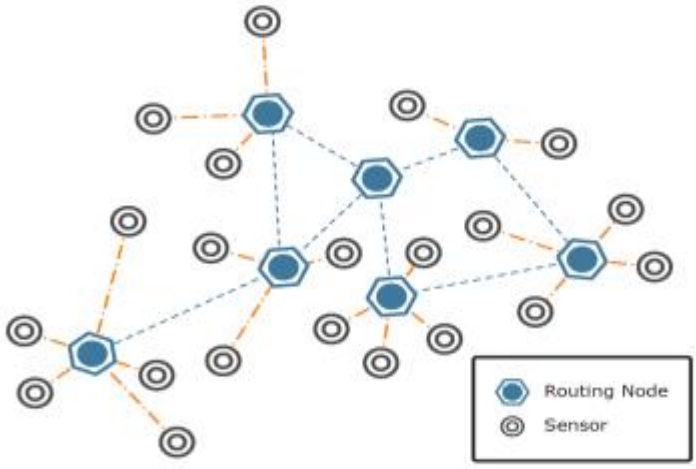

Fig.1.Sensor Network

microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

2. RELATED WORK

A sensor node, also known as a mote (chiefly in North America), is a node in a sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. A mote is a node but a node is not always a mote. Although wireless sensor nodes have existed for decades and used for applications as diverse as earthquake measurements to warfare, the modern development of small sensor nodes dates back to the 1998 Smart dust project and the NASA Sensor Webs Project One of the objectives of the Smart dust project was to create autonomous sensing and communication within a cubic millimeter of space. Though this project ended early on, it led to many more research projects. They include major research centers in Berkeley NEST and CENS. The researchers involved in these projects coined the term mote to refer to a sensor node. The equivalent term in the NASA Sensor Webs Project for a physical sensor node is pod, although the sensor node in a Sensor Web can be another Sensor Web itself. Physical sensor nodes have been able to increase their capability in conjunction with Moore's Law. The chip footprint contains more complex and lower powered microcontrollers. Thus, for the same node footprint, more silicon capability can be packed into it. Nowadays, motes focus on providing the longest wireless range (dozens of km), the lowest energy consumption and the easiest development process for the user. The overall theoretical work on WSNs works with passive, omni-directional sensors. Each sensor node has a certain area of coverage for which it can reliably and accurately report the particular quantity that it is observing. Several sources of power consumption in sensors are: signal sampling and conversion of physical signals to electrical ones, signal conditioning, and analog-to-digital conversion. Spatial density of sensor nodes in the field may be as high as 20 nodes per cubic meter.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 6 (2017) PAGES 2452 - 2456
RECEIVED : 25.10.2017 PUBLISHED : 13.11.2017
Nov 13, 2017

3. IMPLEMENTATION

However, the current trust-based route strategies face in obtaining trust. However, obtaining the trust of a node is very difficult, and how it can be done is still unclear. Energy efficiency. Because energy is very limited in WSNs, in most research, the trust acquisition and diffusion have high energy consumption, which seriously affects the network lifetime. (3) Security. Because it is difficult to locate malicious nodes, the security route is still a challenging issue. Thus, there are still issues worthy of further study. Security and trust routing through an active detection route protocol is proposed in this paper. The main innovations are as follows. The Active is the first routing scheme that uses active detection routing to address BLA. The most significant difference between Active Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will attack these routes and, in so doing, be exposed. I

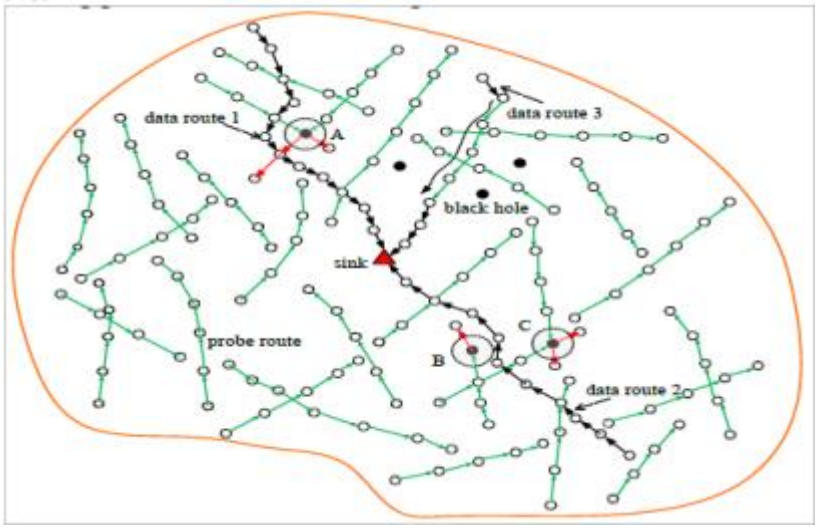

Fig.2.System Architecture

n this way, the attacker's behavior and location, as well as nodal trust, can be obtained and used to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs. The Active Trust route protocol has better energy efficiency. Energy is very precious in WSNs, and there will be more energy consumption if active detection is processed. Therefore, in previous research, it was impossible to imagine adopting such high-energy-consumption active detection routes. However, we find it possible after carefully analyzing the energy consumption in WSNs. Research has noted that there is still up to 90% residue energy in WSNs when the network has died due to the "energy hole" phenomenon. Therefore, the Active Trust scheme takes full advantage of the residue energy to create detection routes and attempts to decrease energy consumption in hotspots (to improve network lifetime). Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security.

4. ANALYSIS

For these tasks run-time is important and turn-around time (run simulation, find bug, fix bug, recompile, re-run) is less important. C++ is fast to run but slower to change, making it suitable for detailed

protocol implementation. A large part of network research involves slightly varying parameters or configurations, or quickly exploring several scenarios. In these cases, iteration time (change the model and re- run) is more important. Since configuration runs once (at the beginning of the simulation), run-time of this part of the task is less important. Tcl runs slower than C++ but can be changed very quickly (and interactively), making it ideal for simulation configuration. Users create new simulator objects through the Tcl interpreter. These objects are instantiated within the interpreter, and are closely mirrored by a corresponding object in the compiled hierarchy.

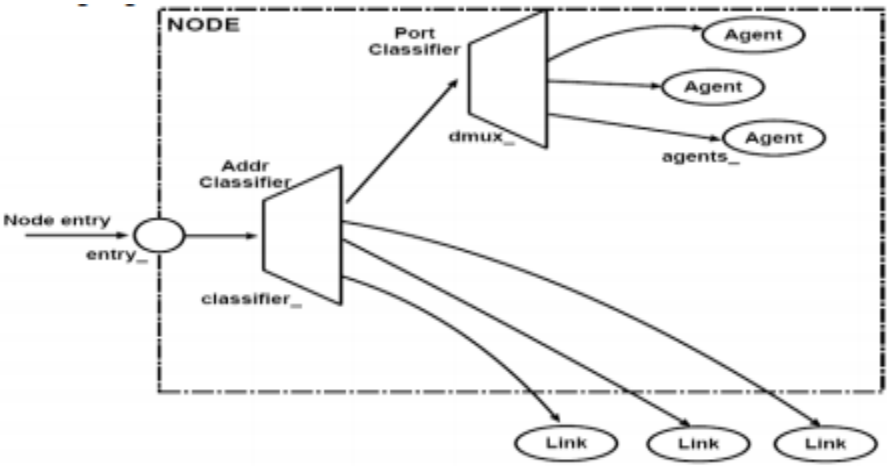

Fig.3.Node Structure

Class TclObject is the base class for most of the other classes in the interpreted and compiled hierarchies. Every object in the class TclObject is created by the user from within the interpreter. An equivalent shadow object is created in the compiled hierarchy. The two objects are closely associated with each other. The interpreted class hierarchy is automatically established through methods defined in the class TclClass. User instantiated objects are mirrored through methods defined in the class TclObject.

CONCLUSION

In this paper, I have proposed a novel security and trust routing scheme based on active detection, andit has the following excellent properties: High successful routing probability, security and scalability. The Active Trust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. High energy efficiency. The Active Trust scheme fully uses residue energy to construct multiple detection routes. The theoretical analysis and experimental results have shown that our scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases. Further, our scheme improves both the energy efficiency and the network security performance. It has important significance for wireless sensor network security.

REFERENCES

1. Aad I. Hubaux P. J. and. Knightly W. E, 2008."Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, vol. 16, no. 4, pp. 791- 802,

2. Dong M., Ota K., Liu A., et al. 2016. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

3. He D. Chen C. , Chan S. Bu J. Vasilakos A. V. 2012. "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 4, pp. 623-632, 33.

4. He Q. , Wu D. , . Sori P. K, 2004."a secure and objective reputation-based incentive scheme for ad hoc networks," IEEE Wireless Communications and Networking Conference, pp. 825–830,

5. Hu .Y, Dong M., Ota K., et al.Doi: 10.1109/JSYST.2014.2308391, 2014. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal,

6. He S., Chen J., Jiang F., et al. (2013) "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931-1942, 2013.