ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 5.015, Special Issue, February 2019 - Conference Proceedings
International Conference on Management 4.0: Disruptions in Business and Millennials at the Workplace (KRUPACON 2018) On 12th & 13th October 2018 Organized By
Krupanidhi Group of Institutions, Bangalore, Karnataka

AN INNOVATIVE METHOD TO SECURE ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

Rajkumar N* & N. Anuradha**
* Krupanidhi Group of Institutions, Bangalore, Karnataka
** Krupanidhi Degree College, Bangalore, Karnataka

Cite This Article: Rajkumar N & N. Anuradha, "An Innovative Method to Secure Routing Protocols in Wireless Sensor Networks", International Journal of Computational Research and Development, Special Issue, February, Page Number 27-29, 2019.

Abstract:

Wireless sensor (WSN) networks have been widely used in recent years, creating important scenarios for equipment security. WSN networks have important limitations such as much less device capabilities, less processing power, controlled power supplies, power limits, body capture responsibilities, and dangerous Wi-Fi chassis networks. Older devices have several issues, including poor overall performance and poor security. This document now reflects the use of lightweight routing protocols to improve neighborhood safety and troubleshooting. Some routing protocols handle basic network errors (e.g. up/down connections, node closures and node startups, etc.), and can also lose significant trust in handling attackers in geographic locations. The most serious attacks are attacks. For this reason, we have proposed a practical and effective multi-float data topology (MDT) routing strategy to protect against this attack, and a series of optimization techniques to reduce energy consumption. Keep your system secure. An effective and successful decision depends on the location of the sensor node in the scheduling operation and the reliability of the target node. Use it for security purposes and select dependent nodes. Therefore, it reduces network life and package success through black hole attacks.

Key Words: WSN, Routing Protocols, Secure Routing Protocol, Network, Security

Introduction:

The use of wireless sensor networks (WSNs) has grown rapidly. The growing interest in network security has accelerated the impressive growth of the Internet. In terms of security, the highest standards for network security have been added, such as Secure Shutdown, Secure Shutdown, Convenient Quality of Service (QoS), and Convenient Community Infrastructure. Device protection is usually achieved by creating a security wall for unmarried hosts, but more recently the firewall era has been used to extend the "security limits" for any company by protecting the intranet with a small set of firewall systems. Convenient routing protocols should be able to detect the presence of harmful characters in society and prevent characters from interfering with routing methods. The path log should choose a path that does not contain such a node, even if such malicious nodes are part of the path. Therefore, we proposed a series of optimization methods to reduce electricity costs, keep the system protection at an appropriate level, effectively design countermeasures based on the equatorial sensor and target node, and consider the lifespan of the group according to the intensity. The network is not enough to send packets. First, let's look at the bandwidth of a node regardless of whether the node is sending packets to nearby nodes. And this saves resources and provides comfort from record-breaking collisions and black hole attacks.

Problem Statement:

The need for wireless sensor networks is faster and more attractive. With a WSN network with many limitations with less computing power, you will no longer have an astonishing number of garage features, controlled energy properties, electrical barriers, legal obligations for eavesdropping, and use of physically unsafe oral Wi-Fi networks. This paper aims to list and defend the answers to some limitations, and several papers cover some public questions. In an open environment, an ignorant sensor node architecture reduces the security and reliability of the sensor network. The motive of this method is that the package is safe and the intermediary packet transmission is not lost when it is transmitted with concern for truth. And using the group's lifetime still saves resources.

Literature Review:

Hu et al. [1] The proposed target tracking scheme. The first is to detect the target with K as the trigger frequency (TDSFK) and detect the target with a configurable trigger frequency (TDASF). It then uses the adjustable rate of fire to identify the target and coordinates the recall to the nearest control node. The success of the proposed plan was evaluated for three parameters: target negligibility, delay potential, and life potential. Here, if the TDASF result falls by more than 17-4%, the life of the system increases and the weighted environment decreases by more than 101.6%.

Dong et al. [2] Estimates the estimation method below the WSN reliability limit to meet the specification of the detection mechanism of all switching points for power consumption with source-to-consumer transmission delay. In fact, the number of confirmations sent increases and the number of statistical messages sent decreases, which reduces the energy consumption of the hub. First of all, in this paper, taking into account the limited efficiency of the Wi-Fi sensor network, we propose an evaluation method to meet the detection of software needs by exchanging (lifetime) energy consumption and delayed transmission from the power supply to the consumer. According to the Send-and-Wait Automatic Search (AR-SW-HBH ARQ) protocol for clustered WSNs, it provides latency and lifetime estimates. Too high reliability in WSN transport connections is an effective solution to unify group reliability using the ARQ protocol. This document reaches the peak of the linear cluster radius, which secures energy consumption and provides theoretical control by delaying the theoretical estimation according to the SW-ARQ protocol. Then I recommend the extended BCMN/A protocol, and the BCMN/A protocol advertises within the cluster and returns multiple ACKs for all data received from the cluster, sending additional ACKs with less overhead. , Send fewer heavy cargo packages and extend this period. purpose. Provide network services, reduce network latency and reduce node energy consumption.

In terms of price competition model, Liu et al. [3] SO increases and decreases the cost of services on a regular basis depending on the scope provided by the organization. It is primarily a leisure-oriented payment selection model (GSPD) that describes payment options. In the GSPD variant, the organization survives the strongest organization, plays sports with other organizations, and measures payments according to their own payment matrix to obtain the ideal Pareto balance factor.

Zhu et al. [4] With a real trust tool combined with popularity measurement and management (ATRCM), and a proven system with reliability with cloud computing (CC) and WSN integrated management. ATRCM provides the following features: Sensor Network Providers (SNPs) and Cloud Service Providers (CSPs) make it possible to bypass malicious impulse attacks. Calculate valid approval with a positive credit rating from the operator. Help cloud provider (CSU) users to choose the right PDC and help the PDC choose the right SNP.

Proposed by Zheng et al. [5] developed an energy efficient cycle-based complete clone detection (ERCD) method to balance efficient traffic load and successful clone detection over long network times. ERCD requires a witness selection and verification layer. To clarify that the witnesses for each sensor node are distributed across the ring system, the protocol can almost detect a clone attack with a capacity of 1, so it is easier to do with a validation message. In addition, the data buffer function suitable for the garage can increase the service life and total energy consumption in the area. This is because it uses regional data using traffic flows.

Due to the load during the WSN, the energy consumption of the sensor node and the memory capacity of the entire receiving node are reduced, and the network life is increased. The protocol also requires additional time to distribute the package instead of using the convenience of an unusual example in other network scenarios.

Zhou et al. [6] Method for watchdog. The theoretical probability of identifying a clone is 100% with the help of a reliable witness. Clonal identification is often studied by fake witnesses. The probability of identifying 98% of the clones found simultaneously with the infected viewer is 10%. In summary, the material presented in this document is that when reviewing current WSN systems (WSNTS), we explicitly identify power contract disputes arising from the successful use of watchdog technology. Previous studies in the literature have no longer comprehensively discussed this conflict, are stepping up defensive body tactics, each with a technical review to identify key potential consequences and a set of practical rules for scheduling body data. Need. Protected and tested accurately and reliably. Optimization method with good management responsibility. Experimental results have effectively proven the effectiveness of the design. The overall goal is to keep electricity bills for monitoring as low as possible while maintaining consistency and reliability in achieving bandwidth.

Han et al. [7] An organized sensor patrol (CSP) algorithm to further improve obstacle protection, extracting a new sensor removal system from the arrival information of previous intruders. CSPs share the sensor frequency and intruder registration, effectively increasing the perimeter range. Average distance the sensor travels from a given point when the PDC's slot is the smallest. Hence, this method has incredible potential to reduce unit cost and provides a whole new and cost-effective alternative to access barrier insurance in large cellular sensor networks. As part of our destiny, we explore the full range of the k-barrier through a network of cellular sensors.

For exchanges outside the center, Seo et al. [8] Notifies the denial of the specified key and reduces the impact of the digest agreement on the security of other communication links. To protect against exceptional attacks, you can assess the security of the program in front of conference participants. Update CL-EKM (Certificate Successful Key Management Protocol) in Contiki OS and emulate it with Cooja to accurately specify time, power, pairing and memory in the system.

Proposed by Zhang et al. [9] introduced payment allocation and data read management (DS2RC) methods to improve common identification and dissemination of statistics while keeping units secure. Low computational complexity allows data to be collected efficiently. Concurrent DS2RC data processing improves register identification and transfer to keep the system secure. In DS2RC, each sensor chooses to adjust the life of the transmission boiler at the heart of the construction process as specified in the life of the achievable port, and to effectively detect and control the charge that fits the set of statistics.

To survive the attack, Sun et al. [10] uses MDT (Multiple Data Flow Topology) system, and BS has the advantage of obtaining statistics at a reasonable time even if the package is lost. In that sense, there are several challenges or problems with the dominant system. Second, MDT (Multivariate Drift Topology) method is used to protect against this attack. There are many advantages to using the MDT system to protect against this attack. The biggest advantage of this is that even if some packages are lost, the downstream station collects statistics on schedule.

Goals:

Here are the goals of the designed tool.

- Reduce sustainability costs while protecting your device at an appropriate level.
- As with the location of the sensor node and the reliability of the target node, data is accurately and efficiently planned.

Proposed Methodology:

Package security is a key issue for the proposed tool and we think about routing throughout the life of the community. Adopt an optimization strategy to reduce energy consumption and maintain adequate device protection. And accurate and successful work plan based on the reliability of the location and address service of the sensor service. And since the strength of the group is often not enough to move the packet, the network lifetime is also important, so first look at the strength of the node if you can't control which packets close the node. And it has the advantage of saving energy, destroying data quickly and attacking black holes.

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 5.015, Special Issue, February 2019 - Conference Proceedings
International Conference on Management 4.0: Disruptions in Business and Millennials at the Workplace (KRUPACON 2018) On 12th & 13th October 2018 Organized By
Krupanidhi Group of Institutions, Bangalore, Karnataka

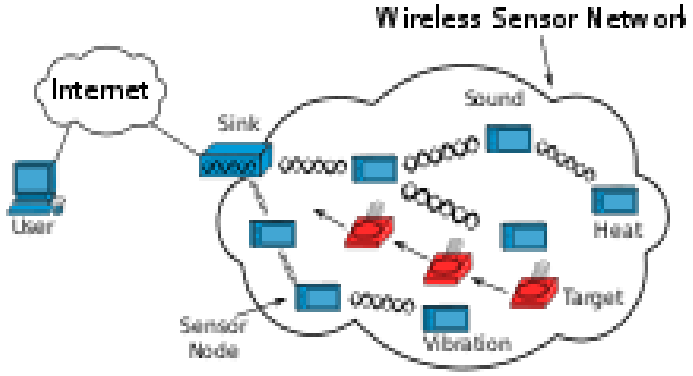

Figure 1: Proposed Methodology

This paper on routing protocol active routes provides security and verifies. The main difference between functional confidence and previous experiments is that they establish multiple detection paths in the region with residual energy. Attackers don't always know the path of detection, so they target specific paths to detect. In this way, in order to prevent the black hole from processing the actual statistical path, it can learn the attacker's behavior and location and use it for targeted operations. As far as we know, this is the first mechanism proposed for active identification in WSNs. We create group keys for the safety of the cars we provide. When receiving a node, there is no community key, so the packet received by this node is not possible, and this node cannot rotate the packet either.

Conclusion:

In this case, a new protection is proposed in the absence of a dedicated router, which is a complex network operation. Various factors that make it difficult to maintain quiet conversations in an ad hoc wireless network include node flexibility, inconsistent behavior, limited node throughput, and limited availability of sources such as capacity, bandwidth, and memory. In this paper, we proposed a new security and considered identity-based routing schemes and active gifts. (1) Efficient routing, security and scalability with high probability. In order to quickly perform optimal routing functions, a successful trust mechanism can quickly determine node trust and then bring down the suspect node. (2) High performance. Active trust uses residual power to create multiple search paths.

Acknowledgement:

The authors express gratitude towards the assistance provided by The Management, Krupanidhi Group of Institutions (KGI) and Krupanidhi Research Incubation Centre, KGI in completing the research. We also thank our Research Mentors who guided us throughout the research and helped us in achieving the desired results.

References:

1. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal, 2014.
2. M. Dong, K. Ota, A. Liu, et al. "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
3. X. Liu, M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198, 2016.
4. C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.
5. Z. Zheng, A. Liu, L. Cai, et al. "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks," IEEE Transactions on Mobile Computing, Vol. 15, no. 5, pp. 1130-1143, 2016.
6. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.
7. S. He, J. Chen, X. Li, et al. "Mobility and intruder prior information improving the barrier coverage of sparse sensor networks," IEEE transactions on mobile computing, vol. 13, no. 6, pp.1268-1282, 2015.
8. S. H. Seo, J. Won, S. Sultana, et al. "Effective key management in dynamic wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2014.
9. Y. Zhang, S. He, J. Chen. "Data Gathering Optimization by Dynamic Sensing and Routing in Rechargeable Sensor Networks," IEEE/ACM Transactions on network, 2015.
10. H.Sun, C. Chen, Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. Of IEEE TENCON 2007, pp. 1-4, 2007.
11. Z Ling Liu, Weisong Shi," Trust and Reputation management" in IEEE Internet Computing, pp.1089-7801, 2010.