JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 5, ISSUE 06, 2018

IdentifyNode Clones in Mobile Wireless Networks Using Fuzzy BasedImplementation

Bhupesh Deka[1], Sitanath Biswass[1], N. V. N. Sowjanya[2]

[1, 2]Assistant Professor,[1,2]Dept. of CSE

[1]Gandhi Institute for Technology, Bhubaneshwar,[2]Siddhartha Institute of Technology and Sciences Hyderabad

Abstract

An efficient detection and recovery algorithm to identify clone node efficiently to recover the Wireless Sensor Networks by replacing only few sensor nodes along with often used alternative routes. Wireless sensor networks areexposed to different types of security threats is reduce the performance of the total network. Defensive mechanisms like key management protocols, authentication protocols and secure routing is providing security to WSN. We first analyze the desirable properties of a distributed model. After that we show the solutions for the problem and later for detection of node replication attacks. We propose a self-healing RED protocol Randomized, Efficient, and Distributed protocol.We propose a technique to improve routing protocols by considering both energy and failure constraints and managing the proposed protocol, the routing protocols dynamically modify to node's failure. We propose a fuzzy based efficient routing protocol (FBERP) for large scale mobile networks that aims to minimize the packet loss rate. Every node in the network is characterized by its communication parameters. We develop a fuzzy logic controller that combines these parameters, Packet Loss Rate, Communication Rate, Energy and Delay Parameters.

***Index Terms**: Distributed Solutions, Physical Capture Attacks, Wireless Sensor Networks, Security, Intrusion Detection System, Fuzzy Logic, Route Recovery, Route Discovery.*

1. Introduction

A wireless sensor network consists of spatially tribute autonomous sensors to monitor physical conditions in wireless sensor networks is deployed in harsh environments to fulfill both military and civil applications [1]. A Wireless Sensor Network (WSN) is a highly distributed network of resource constrained and wireless devices arecalled sensor nodes. Each sensor node modifies some physical phenomenon inside the area of deployment [2]. The collected measurement is sent to a base station. The communication range of sensor nodes is limited to tens of meters and directly communicates with the base station [3]. The Wireless sensor network is a collection of sensors is spread over large geographic area. Since sensors is widely spread and large in number the occurrences of faults in the network.

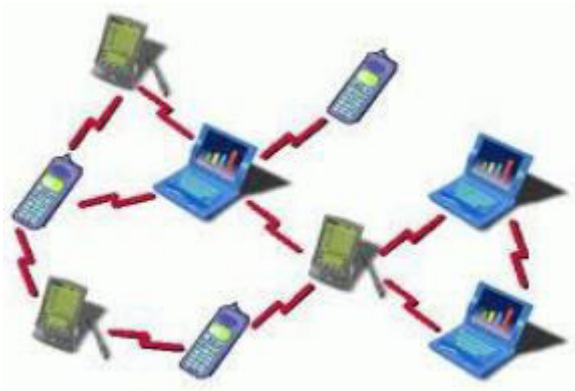

Figure 1. Mobile network

ISSN- 2394-5125 VOL 5, ISSUE 06, 2018

Hence to detect the fault node and to replace the fault node an efficient algorithm is proposed [4]. Fuzzy logic implements human experiences and preferences via membership functions and fuzzy rules. A membership function is a mathematical formation of representing a fuzzy set [5]. A fuzzy number is a quantity total value is imprecise rather than exact as is the case with "ordinary" numbers [6].

2. Related Work

Failures are unavoidable in Wireless Sensor Networks due to the lack of updating and unattended deployment. There are many methods related to energy, memory and computational ability of a sensor node. The occurrences of faults are mostly due the presence of faulty sensor nodes [7]. To identify a fault node and to replace it many techniques is proposed [8]. Most of the sensor network applications used reliable data delivery to sink instead of point-to-point reliability. It is vital to provide fault tolerant techniques for distributed sensor network applications [9]. The metrics find Link Expiration Time (LET), Received Signal Strength (RSS), Available Bandwidth (ABW) and Residual Energy (RE) and based on these metrics' node is classified as weak, normal or strong using fuzzy set[10]. Proposed distributed routing protocol TORA is provides functions, Creation of routes, Maintenance of routes and Erasing of routes. The protocol uses different packets for these functions [11].The same results show that the proposed RED protocol meets the desirable properties. We find the feasibility of the RED protocol. The set of simulations result shows the RED protocol is implemented in sensor network is analyzed [12]. And, as a self-healing model it used continuously iterated over the same network without significantly affecting the detection protocol and network performance itself. We consider the influence of an attacker intervening on message routing both for RED and LSM [13].

3. Threat Model

It replicates one or more clones into multiple copies by compromising a certain fixed number of nodes. In general, it is possible to cope with threat to assume that nodes are tamper-proof. We will assume that the nodes do not have tamperproof components consistently with a large part of the tamper-proof hardware is expensive and energy demanding [14]. To prevent clones from being detected by the detection protocol used in the mobile network is the adversary goal. The sensors choosing from the total network is compromised by adversary. Intuitively an adversary that needs some time to move from one point to another of the network area is described by the localized adversary, while the ubiquitous adversary security nodes regardless of their position during the same time interval [15].

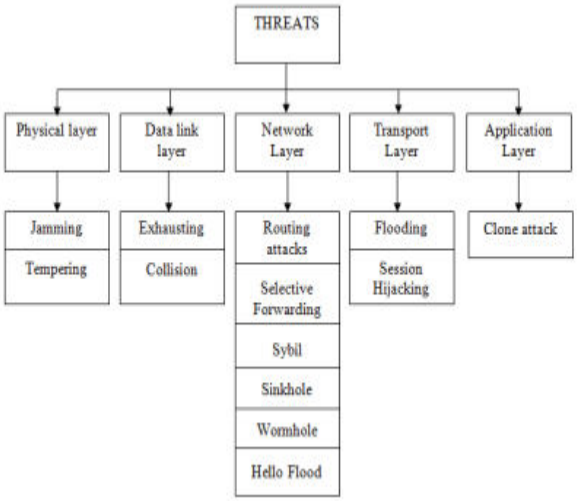

Figure 2. Layer based classification of threat

ISSN- 2394-5125 VOL 5, ISSUE 06, 2018

4. Proposed System

Our mobile network model takesset of low-power radio frequency (RF) transceivers which move relative to each other across an irregular terrain subject to RF propagation impairments. The combination of low power and propagation environment produces a network characterized by stochastic link failures. We propose a novel scheme Link Scanner (LS) for updating wireless links at real time [16] We propose a self-healing RED protocol. Randomized, Efficient. Distributed protocol and it meets the requirements. Finally, it shows that our protocol is highly efficient in memory, communication and computation. The mobile robots check the group of sensor functions and exchange secret keys and verify their identities. Upon new inclusion, a node is collecting enough authorizations from its neighbors and privilege is accepted by the sink [17] . The presence of unauthorized node is detected by Bootstrapping algorithm. Bootstrapping the sensor network refers to the discovery of deployed sensors and finding direct communication links between each gateway and sensors that are reachable to it. We propose a fuzzy based efficient routing protocol (FBERP) for large scale mobile networks that aims to minimize the packet loss rate. Each node in the network is characterized by its communication functions develop based on fuzzy logic [18].

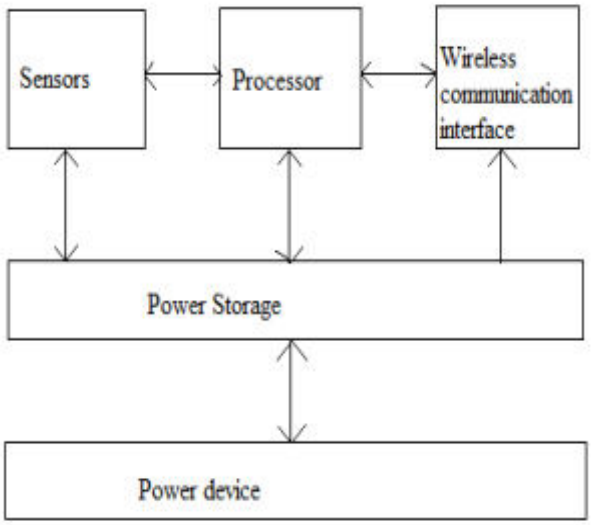

Figure 3. Block Diagram of Mobile Network

4.1. Grade Diffusion Algorithm

The Grade Diffusion algorithm not only creates the routing for each sensor node is also identifies a set of neighbor nodes to reduce the transmission loading. Each sensor node is select a sensor node from the set of neighbor nodes relay. The number of sensor nodes is functioning exceeds the threshold [19]. Genetic algorithm is used for replacement [20]. There are 5 steps in the genetic algorithm: Initialization, Evaluation, Selection, Crossover, and Mutation

Initialization: Here chromosomes is generated. Each Chromosome is an expected solution. The number of chromosomes depends on number of sensors is replaced.

Evaluation: The Number of routing path available some nonfunctioning sensors is replaced evaluated based on fitness value. This fitness value is calculated with number of sensor nodes grade values, number of reusable routing paths.

Selection: Here chromosomes with lowest fitness values are eliminated.

Cross over: Two individual chromosomes is selected and compared and a part of it is replaced with the other to produce new offspring.

Mutation: Here a single gene is replaced after comparison.

ISSN- 2394-5125 VOL 5, ISSUE 06, 2018

4.2. Fuzzy Based Efficient Routing Protocol

We propose new fuzzy based efficient routing protocol (FBERP) for large scale mobile networks that aims to minimize the packet loss rate. Every node in the network is characterized communication parameters [21]. We develop a fuzzy logic controller that combines these functional Packet Loss Rate, Communication Rate, Energy and Delay Parameters. The value obtained, indicates the priority of a node with maximum throughput is selected and it is used in route formation. Our simulation of proposed protocol outperforms the standard AOMDV routing protocol as the packet loss rate is minimized in our proposed work. In future work can be done to lower down the packet delay and any other communication parameters may be used to further improve the protocol [22].

4.3. Algorithm

Step 1: N nodes is distributed in network.

Step 2: Initially all nodes conserve same energy.

Step 3: Each packet sensed by a node is assigned a unique number id & broadcast it to all nodes in the network.

Step 4: Each node that receives the id checks if it is already stored in its memory.

Step 5: If yes, the data will be discarded.

Step 6: Else, select the higher residual energy node with the shortest distance path.

Step 7: Else if node with same residual energy and distance then packets is transmitted with higher timestamp value.

Step 8: Maintain the location information of node and continue the same process till destination found.

Step 8: If packets collision occurs then reduce the contention window by giving the priority to node with higher residual energy.

Step 9: check whether the data reach to the destination

Step 10: If yes, broadcast the packet id to all nodes

5. Results

Network density is significantly changing the network topology. A dense network should suffer more channel collision and packet lost due to hidden terminal, thus may impact the probe flooding process and cover the real link results. We used NS2 to simulate our proposed protocol. In our simulation the packet interval is set to be 0.0008sec. We use IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer in link breakage. In our simulation, 25 mobile nodes move in a 500×500 m region for 10 seconds simulation time. We assume each node moves independently with the same average speed. In our simulation, the simulated traffic is TCP (ftp).Our simulation settings and parameters are summarized.

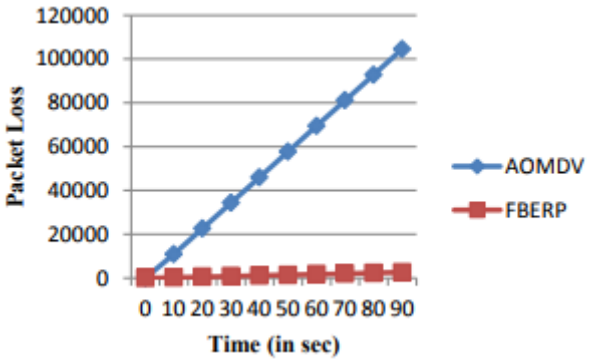

Figure 4. Packet delay

ISSN- 2394-5125 VOL 5, ISSUE 06, 2018

6. Conclusion

The detection of node replication attacks We first analyzed the desirable properties of a distributed mechanism. The Efficient fault detection and recovery algorithm is identifying a fault node when some of the sensor nodes shut down, either because they no longer have battery energy or they have reached their operational threshold but also when an unauthorized sensor got included in the network. We develop a fuzzy logic controller that combines functions, Packet Loss Rate, Communication Rate, Energy and Delay Parameters. The value obtained, indicates the priority of a node; a node with maximum throughput is selected and it is used in route formation. Also try to further reduction of load in the network by increasing the lifetime of the network.

References

[1] R. Badonnel, R. State, and O. Festor. Self-configurable fault monitoring in ad-hoc networks. Ad Hoc Networks, 6(3):458–473, May 2008.

[2] P. Inverardi, L. Mostarda, and A. Navarra, "Distributed IDSs for enhancing Security in Mobile Wireless Sensor Networks," in Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on, 2006, pp. 116-120.

[3] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," Communications Surveys & Tutorials, IEEE, vol. 8, pp. 2-23, 2006.

[4] Rehena, Z.; Das, D.; Roy, S.; Mukherjee, N., "Handling area fault in multiple-sink Wireless Sensor Networks," Advance Computing Conference (IACC), 2013 IEEE 3rd International , pp.458-464, 2013.

[5] Justin Yackoski, Chien-Chung Shen, Cross-layer Inference-based Fast Link Error Recovery for MANETs, WCNC 2006 proceedings, 1-4244-0270- 0/06/(c)2006 IEEE, PP 715-722, 2006.

[6] A Naga Raju, Dr. S Rmachandram, Fuzzy Cost Based Multipath Routing for Mobile Ad-Hoc Networks, Journal of Theoretical and Applied Information Technology, PP 319-326, 2008.

[7] Ting Yang, Yugeng Sun, Javid Taheri and Albert Y. Zomaya, " DLS: A dynamic local stitching mechanism to rectify transmitting path fragments in wireless sensor networks," Journal of Network and Computer Applications, vol.36, pp. 306– 315,2013.

[8] PrasenjitChanak, TuhinaSamanta and Indrajit Banerjee, "Fault – Tolerant multipath routing scheme for energy efficient Wireless Sensor Networks," International Journal of Wireless & Mobile Networks, vol. 5, No. 2, pp. 33-45, 2013.

[9] T. H. Liu, S. C. Yi, and X. W. Wang, "A Fault Management Protocol for Low-Energy and Efficient Wireless Sensor Networks," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, No. 1, pp. 34-45, 2013.

[10] Khalid Zahedi, Abdul Samad Ismail, Route Maintenance Approach for Link Breakage Predicttion in Mobile Ad Hoc Networks, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 10, PP 23-30, 2011.

[11] Arash Dana, GolnooshGhalavand, AzadehGhalavand, FardadFarokhi, A Reliable routing algorithm for Mobile Adhoc Networks based on fuzzy logic, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, ISSN (Online): 1694-0814, PP 128-133, May 2011.

[12] C. Cocks, "An Identity Based Encryption cheme Based on Quadratic Residues," Proc. IMA Int'l Conf. '01, pp. 360-363, 2001.

[13] M. Conti, R. Di Pietro, A. Gabrielli, L.V. Mancini, and A. Mei, "The Quest for Mobility Models to Analyse Security in Mobile Ad Hoc Networks ,"Proc. Seventh Int'l Conf. Wired/Wireless Internet Comm. (WWIC '09), pp. 85-96, 2009.

[14] M. Conti, R. Di Pietro, and L.V. Mancini, "Secure Cooperative Channel Establishment in Wireless Sensor Networks," Proc. IEEE Pervasive Computing and Comm. (PERCOM '06) Workshop, pp. 327- 331, 2006.

[15] M. Conti, R. Di Pietro, and L.V. Mancini, "ECCE: Enhanced Cooperative Channel Establishment for Secure Pair-Wise Communication in Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 49-62, 2007.

[16] Pooja, Ajay Dureja, Enhancement of Multipath Routing Protocol for Route Recovery in MANET, European Scientific Journal, ISSN: 1857-7881 (Print) e-ISSN 1857-7431, edition vol.9, No.18, PP 270-281, June 2013.

[17] Devi M., V. RhymendUthariaraj, Congestion Based Route Recovery Technique for MANET, Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, E-ISSN: 1817-3195, Vol. 54 No.1, PP 73-81, August 2013.

[18] Sara Aliabadi, Mehdi Agha Sarram, An Improvement on Route Recovery by Using Triangular Fuzzy Numbers on Route Errors in MANET, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278- 0661, p- ISSN: 2278-8727, Volume 16, Issue 1, Ver. II, PP 75-79, January 2014.

ISSN- 2394-5125 VOL 5, ISSUE 06, 2018

[19] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"Wireless sensor networks: a survey,"Computer Networks , vol.38 , pp.393–422 ,2002.

[20] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H and Subir Kumar Sarkar, " Issues in Wireless Sensor Networks" Proceedings of the World Congress on Engineering , vol. 1, 2008.

[21] Manveen Singh Chadha, RambirJoon, Sandeep, Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[22] P. Periyasam, Dr. E. Karthikeyan, Performance Evaluation of AOMDV Protocol based on Various Scenario and Traffic Patterns, International Journal ofComputer Science, Engineering and Applications (IJCSEA), Vol.1, No.6, PP 33-48, December 2011.