International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-7)

Research Article

July 2015

Enhanced WSN Transmission Scheme using Fuzzy based Swarm Intelligence Approach

Shivani Jindal
Computer Science and Engineering, Kurukshetra University,
Kurukshetra, Haryana, India

Abstract—

One of the main challenges in wireless sensor networks is to provide low-cost, low-energy reliable data collection. Reliability against transient errors in sensor data can be provided using the model-based error correction, in which temporal correlation in the data is used to correct errors without any overheads at the sensor nodes. In the above work it is assumed that a perfect model of the data is available. However, as variations in the physical process are context-dependent and time-varying in a real sensor network, it is infeasible to have an accurate model of the data properties a priori, thus leading to reduced correction efficiency. In this paper, we address this issue by presenting a scalable methodology for improving the accuracy of data modelling through fuzzy based model updates. Additionally, we propose enhancements to the data correction algorithm to incorporate robustness against dynamic model changes and potential modelling errors. We evaluate our system through simulations using real sensor data collected from different sources. The proposed work is implemented on the MATLAB.

Keywords— WSN (Wireless sensor networks), QOS (Quality of service), DOS (Denial of service), TCP (Transmission control protocol), PSO (Particle swarm optimization) etc.

I. INTRODUCTION

The convergence of techniques for sensing, communication, and processing has led to the emergence of wireless sensor networks. One of the goals of the wireless sensor networks is to enable reliable data collection to meet the goals of the applications. Providing reliability is an important issue to address because majority of the sensor networks are remotely operated with very little human intervention once deployed and the maintenance/repair is also infeasible at times. Additionally, the sensor network is inherently exposed to several sources of unreliability such as errors from hardware noise, communication errors, errors in sensors, etc., necessitating the need for reliability mechanisms.

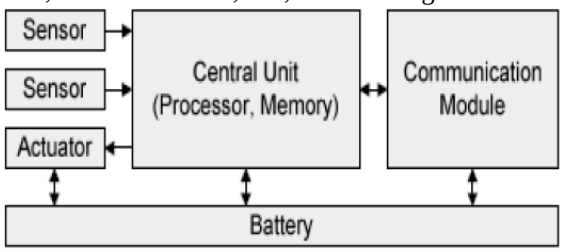


Fig. 1Structure of Sensor Node

Wireless sensor networks are composed of hundreds of thousands of tiny devices called nodes. A sensor node is often abbreviated as a node. What is a Sensor Node? A Sensor is a device which senses the information and passes the same on to a mote. Sensors are used to measure the changes to physical environment like pressure, humidity, sound, vibration and changes to the health of person like blood pressure, stress and heartbeat. A Mote consists of processor, memory, battery, A/D converter for connecting to a sensor and a radio transmitter for forming an ad hoc network. A Mote and Sensor together form a Sensor Node. The structure of the sensor node is as shown in fig 1.

One of the important factors to be considered in providing reliability in large sensor networked systems is the overall deployment cost. The deployment cost can be reduced by using low-cost sensor nodes; however that leads to constrained computational resources available on the sensor nodes. Another factor that affects the deployment of sensor networks is the lifetime of operation is primarily governed by the limited energy resources available. Hence, reliable sensor data collection should be provided using low-cost sensor nodes while consuming very low energy to enable proliferation of large-scale sensor networks.

II. VULNERABILITIES

The vulnerabilities of Wireless sensor network are summarized below

A. Wireless links

First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks.

B. Dynamic topology

Wireless nodes can leave and join the network, and move independently. As a result, the network topology can change frequently. It is difficult to differentiate normal behavior of the network from anomaly/malicious behavior in this dynamic environment.

C. Co-cooperativeness

Routing algorithms for wireless network usually assume that nodes are cooperative and non-malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications.

D. Lack of clear line of defence

WSNs do not have a clear line of defense; attacks can come from all directions. The boundary that separates the inside network from the outside world is not very clear on WSNs.

E. Limited resources

Resource constraints are a further vulnerability. There can be variety of devices on WSNs, ranging from laptops to handheld devices such as PDAs and mobile phones. These will generally have different computing and storage capacities that can be the focus of new attacks.

III. ATTACKS

WSNs often experience unusual security attacks because of their following features such as dynamically changing topology, lack of central monitoring, mutual algorithms and absence of a centralized certification authority etc. Generally mobile ad hoc networks are affected by two kinds of attacks which are classified as passive and active. Passive attacks do not affect the functionality of network, but may attempt to find out vital information by listening to traffic. It is difficult to identify such attacks as under these attacks the network operates normally. These attacks basically obtain critical routing information through sniffing. Such attacks are usually complex to identify and protection against such attacks is also difficult. Moreover, it is sometimes not even possible to trace the exact location of the attacker node. Generally, such type of attacks is prevented with the help of encryption.

LAYERS	ATTACKS
Application layer	Data corruption, viruses and worms
Transport layer	TCP/UDP SYN flood
Network layer	Hello flood, black hole, worm hole
Data link layer	Monitoring, traffic analysis
Physical layer	Eavesdropping, active interference

IV. PROPOSED APPROACH

A. Approach

1) *Quantitative Approach:* This approach is used when the researchers' wants verify the theories they proposed, or observe the information in greater detail.
2) *Qualitative Approach:* This approach follows the strategies such as ethnographies, phenomenology and grounded theories. When the researchers want to study the context or focusing on single phenomenon or concepts then they used qualitative approach to achieve their desired goals.

B. Our Proposed Method

In our proposed work we have used both quantitative and qualitative approaches. This approach starts by studying the elated literature specific to security issues in WSNs and Manet's literature review is followed by simulation modeling. The results are gathered and analysed and conclusions are drawn on the basis of the results obtained from simulation. The proposed work contributes the analysis in the Tabular form to give a clear comparison between various parameters and techniques.

C. Problem Identification and Selection

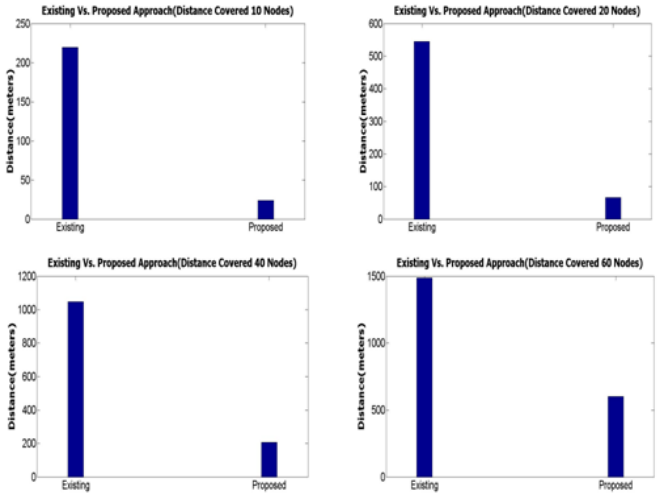
The most important phase is when, it is important to select the proper problem area. Different areas are studied with in mind about the interest of the problem faced and challenges in the network. Most of the time is given to this phase to select the wireless network issue. The proposed work selected WSN as the area of interest and within the network focus was given to the security issues and to counter measure the same. The proposed work is based on the Particle swarm intelligence approach which optimizes the path covered from source to destination and ignores the path if it is affected by any malicious nodes. Thus securing a network based on swarm technique results in optimizes the route. Further the implementation of fuzzy terminates the iteration to the best value.

D. Proposed Algorithm

Algorithm
{
Hop count=0;
Path length =0;
Reachability =0;
For attack node (percentage) =0:1:100
{
For source = 1to N-1
{
For destination= source + 1 to N
{
For iteration 1 to 30
{
Distribute node randomly
If (path exist=y)
{
Calculate
Path length=total distance from S to D;
Hop count= number of intermediate nodes;
Reachability =reachability+1;
PDR=total packets/total nodes;
Efficiency=delivered packets/available packets;
Simulation time= total distance/speed;
}
}
}
}
Average reachability= (2*reachability/N (N-1)*25);
AVERAGE PATH length= path length/reachability;
Average hope count=hop count/ reachability;
}
}

V. SIMULATION RESULT

The code is developed in MATLAB using Fuzzy PSO for different parameters and executed for different sizes of network. The results obtained by proposed algorithm are presented for comparative analysis with previous approach for different number of nodes. We analysed that the proposed approach gives a better result in terms of route optimizations and energy as compared to existing work. Further in section5.1 we compare the proposed approach with the existing approach in terms of distance and energy parameters. The figures 5.4(a-f) are showing the results obtained by existing approach as well as the proposed approach. The network taken is of different number of nodes. As we can see the proposed approach has optimized routes. Hence, our proposed FSO approach for the route optimization in Wireless sensor network gives better results as compared to the existing work.



VI. CONCLUSIONS

In this thesis, we have considered the routing approaches in WSN mobile ad hoc networks from the security and congestion viewpoint. We have analysed the threats against ad hoc routing and presented the requirements that need to be

addressed for secure routing. Existing secure routing algorithm for mobile ad hoc networks are not much secure. And importance of Mobile networks cannot be denied as the world of computing is getting portable and compact. In this present work, we have defined a fuzzy based PSO improved safe routing approach to transfer data from congestion free and attack safe path. Generally, the shortest path is the most favourite area for the attackers to perform the intrusion, but the presented approach will not cover any node that is having the higher probability of the attack or the congestion. As the communication will be performed over a congestion free path, the energy and the delay over the network will be reduced.

ACKNOWLEDGMENT

The writing of this dissertation has been assisted by the generous help of many people. I feel that I was very fortunate to receive assistance from them. I wish to express my sincere appreciation to them.

First and foremost, I am indebted to my principal supervisor, Er Shakti Arora, HOD (CSE), Geeta Engineering College, Naultha, Panipat who has been very supportive at every stage of my dissertation. I wish to express my utmost gratitude to him for his invaluable advice and patience in reading, correcting and commenting on the drafts of the dissertation and, more importantly, for his generosity which I has received throughout my entire research program.

I would like to acknowledge and extended my heartfelt gratitude to our dissertation in-charge who helped and encouraged me throughout this journey.

I wish to express my thanks to all staff members of Geeta Engineering College, Naultha, Panipat, who also helped me in conducting this study.

Finally, I am particularly indebted to my dearest parents/guardians as without their generous assistance and love; this dissertation could never have been completed.

REFERENCES

[1] Y. Hu, D. Johnson, A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02).

[2] Y. Hu, A. Perrig, D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002).

[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, "System architecture directions for network sensors", ASPLOS 2000.

[4] J. Staddon, D. Balfanz, G. Durfee, "Efficient Tracing of Failed Nodes in Sensor Networks", First Workshop on Sensor Networks and Applications, WSNA'02, Atlanta, Georgia, USA.

[5] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[6] Edoardo Amaldi, Antonio Capone, Federico Malucelli and Carlo Mannino, "Optimization problems and models for planning cellular networks",Handbook of optimization in Telecommunications, 2006, 917-939.

[7] Susmi Routray, A. M. Sherry, and B. V. R. Reddy, "Bandwidth Optimization through Dynamic Routing in ATM Networks: Genetic Algorithm & Tabu Search Approach", International Journal of Electrical and Computer Engineering 1(2006), 176-182.

[8] Hao Mei, Yantao Tian and Linan Zu, "A Hybrid Ant Colony Optimization Algorithm for Path Planning of Robot in Dynamic Environment", International Journal of Information Technology, 12(2006), 78-88.

[9] Trevor Davies, "Path Planning and Trajectory Control of Collaborative Mobile Robots Using Hybrid Control Architecture", Royal Military College of Canada (Canada), 2007, 167.

[10] Luc Hogie, "Mobile Ad Hoc Networks: Modelling, Simulation and Broadcast based Applications", European Ph.D Thesis in Computer Science, University of Le Havre (France), 2007.

[11] Weber, Gerhard-Wilhelm and Tezel, Aysu, "On Generalized Semi-Infinite Optimization of Genetic Networks", An official Journal of the Spanish Society of Statistics and Operations Research, 15(2007), 65-77(13).

[12] Mustafa AL-Ghazal, Ayman EL-Sayed and Hamedi Kelash, "Routing Optimization using Genetic Algorithm in Ad Hoc Networks", IEEE International Symposium on Signal Processing and Information Technology, 2007, 497-503.

[13] Alireza Fasih, "Cellular Neural Network Trainer and Template Optimization for Advanced Robot Locomotion, Based on Genetic Algorithm", 15th International Conference on Mechatronics and Machine Vision in Practice, 2008, 317-322.

[14] P. Sateesh Kumar and S. Ramachandram, "Load Balancing in Genetic Zone Routing Protocol for MANETs", World Academy of Science, Engineering and Technology, 35(2009), 517-522.

[15] Jiann-Horng Lin and Li Ren Huang, "Chaotic Bee Swarm Optimization Algorithm for Path Planning of Mobile Robots", 10th WSEAS international conference on evolutionary computing, 2009, 84-89.

[16] Awais Iqbal, "Increasing localization precision in sensor networks with mobile beacons a genetic path planning approach", Technical Report submitted for M.S. Thesis, University of Texas at Arlington, 2009.

[17] M. Bheemalingaiah et al. "Energy aware node disjoint multipath routing in mobile adhoc network", Journal of Theoretical and Applied Information Technology, 5(2009), 416-431.

