Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.169 – 174

A Review on Various Routing Algorithm in WSN

[1]Sunny Kumar, [2]Dr. Anuj Sharma
[1]M.Tech Scholar, Computer Science and Engineering Department, OM Institute of technology and Management, Juglan (Hisar)-125001
[2]Associate Professor, Computer Science and Engineering Department, OM Institute of Technology and Management, Juglan (Hisar)-125001
[1] panwar.sunny51@gmail.com, [2] anuj.k.er@gmail.com

Abstract - A survey of trust and reputation systems in various domains is conducted, with more details given to models in MTR and wireless sensor networks as they are closely related to each other and to our research interests. The methodologies used to model trust and their references are presented. The survey states that, even though researchers have started to explore the issue of trust in wireless sensor networks, they are still examining the trust associated with routing messages between nodes (binary events). However, wireless sensor networks are mainly deployed to monitor events and report data, both continuous and discrete. This leads to the development of new trust models addressing the continuous data issue and also to combine the data trust and the communication trust to infer the total trust.

Key points: WSN, AODV, MTR, MATLAB, PDR.

1. INTRODUCTION

Wireless sensor networks (WSNs) in recent years, have shown an unprecedented ability to observe and manipulate the physical world, however, as with almost every technology, the benefits of WSNs are accompanied by a significant risk factors and potential for abuse. So,

someone might ask, how can a user trust the information provided by the sensor network? Sensor nodes are small in size and able to sense events, process data, and communicate with each other to transfer information to the interested users [1].

Typically, a sensor node consists of four sub-systems.

• Computing sub-system (processor and memory): responsible for the control of the sensors and the execution of communication protocols.

• Communication sub-system (transceiver): used to communicate with neighboring nodes and the outside world.

• Sensing sub-system (sensor): link the node to the outside world.

• Power supply sub-system (battery): supplies power to the node.

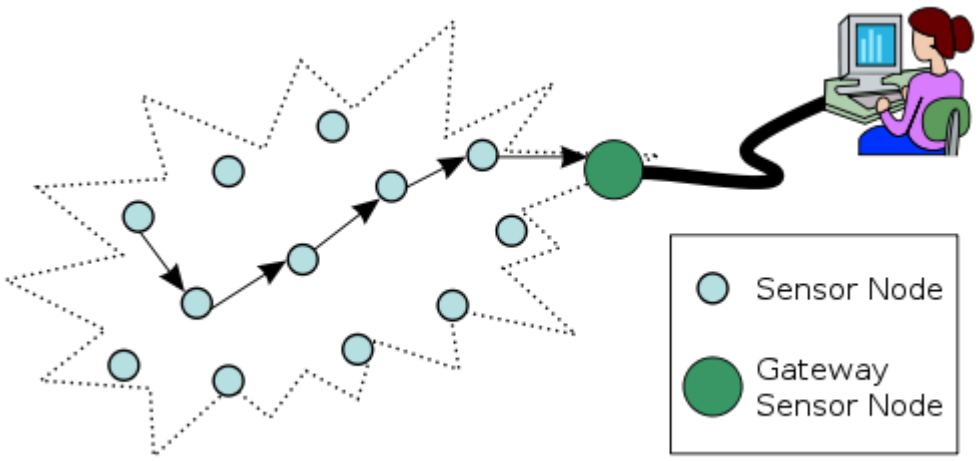

Figure. Wireless Sensor Network

Characteristics of Wireless Sensor Networks

- A WSN typically consists of a large number of low-cost, low power, and multifunctional nodes
- Power consumption constrains for nodes using batteries
- Some mobility of nodes for highly mobile nodes see MWSNs

- Heterogeneity of nodes
- Scalability of large scale of development
- Ease to use
- Ability to with stand harsh environmental conditions
- Ability to cope with node failure (resilience)

Application of WSN

- Nuclear, biological and chemical attack detection and reconnaissance
- Reconnaissance of opposing forces and terrain
- Forest fire detection
- Flood detection
- Military applications
- Health applications
- Targeting
- Battlefield surveillance

2. Literature Review

Security and Integrity Aware Deep Learning Based Approach for Wireless Communications.

The Underwater Acoustic Based Networks are vulnerable and susceptible towards number of natural as well as technical aspects which consume huge amount of energy and therefore it affects the lifetime. A number of approaches are devised so far for the enhancement of lifetime and performance factor of underwater networks, still there is huge scope of research. In this research work, a novel and effective integration of deep learning for energy optimization and performance enhancement is proposed to be implemented [6]. The results in the work depict the proposed approach effectual and optimized in assorted parameters. This work focus on the integration of cloud technologies so that the detailed log of communication can be established, trained and then predictive analytics can be done.

Secure Trust Based Key Management Routing Framework for Wireless Sensor Networks.

Security is always a major concern in wireless sensor networks (WSNs). Several trust based routing protocols are designed that play an important role in enhancing the performance of a wireless network. However they still have some disadvantages like limited energy resources, susceptibility to physical capture, and little protection against various attacks due to insecure wireless communication channels. This paper presents a secure trust based key management (STKF) routing framework that establishes a secure trustworthy route depending upon the present and past node to node interactions. This route is then updated by isolating the malicious or compromised nodes from the route, if any, and a dedicated link is created between every pair of nodes in the selected route with the help of "*q*" composite random key pre-distribution scheme (RKPS) to ensure data delivery from source to destination. The performance of trust aware secure routing framework (TSRF) is compared with the proposed routing scheme [5]. The results indicate that STKF provides an effective mechanism for finding out a secure route with better trustworthiness than TSRF which avoids the data dropping, thereby increasing the data delivery ratio. Also the distance required to reach the destination in the proposed protocol is less hence effectively utilizing the resources.

3. Objective

Objective is to design a trust based effective and efficient security algorithm for WSN.

1. To study various security issues in WSN and various techniques to secure WSN.
2. To propose or modify existing algorithm i.e. MTR (multi-valued trust based routing) to improve the reliability of existing AODV (Ad hoc on-demand distance vector) routing protocol algorithm without compromising its performance.
3. To implement the proposed algorithm using MATLAB and analyze the performance.
4. Compare the performance of modified MTR and existing MTR by using parameter like PDR, end 2 end delay, Throughput, Energy consumption.

4. Research Methodology

Improve the reliability of existing algorithm AODV and modify existing algorithm i.e. MTR without mitigating its performance. Improve performance and implement the proposed algorithm

using MATLAB. Research Work is using MATLAB Simulink environment. In simulation process the mathematical formulation are performed and plotting of mathematical formulation in graphic view. MATLAB (matrix laboratory) is developed by Math works. MATLAB is an numerical computing. MATLAB also interfaced with programming languages like C, C++ etc.

For ″MTR″ also, we are using a 500 × 500 network of 70 sensor nodes for simulation using MATLAB. Let 40% nodes be the advanced nodes taking that are more than the previous algorithm nodes. Now we try to use Wireless Sensor Network (WSN) to modify existing algorithm i.e. MTR (multi-valued trust based routing) to improve the reliability of existing algorithm without compromising its performance and that can be improved interpreted in a list of security requirements, and having a number of sensor nodes connected among them-selves by a wireless medium to perform distributed sensing tasks, which can be used in different types of applications such as surveillance, environmental and health monitoring, and security. Sensor networks are a sensing, computing and communication infrastructure allowing to instrument, observe, and respond to phenomena in the natural environment, and in our day to day life physical and cyber infrastructure. An important aspect of WSNs comes from as for the same set of events it has many sensors generating sensing data.

5. Conclusion

In the previous paper we can find the trusted path but not the shortest. So, in the research paper I am find out the shortest and the trusted path also. In the research paper I am used the MTR (multivalued trust level routing) algorithm to find out the shortest path.

References

[1] Mohammad Momani , SubhashChallaet “Survey of Trust models in Different Network Domain”, 2010

[2]Omid Naderi, Mahdi Shahedi “A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks”, 2015

[3] Renyong Wu, Xue Deng, Rongxing Lu, and Xuemin (Sherman) Shen “Trust-Based Anomaly Detection in Emerging Sensor Networks”, 2015

[4] A.Senthilkumar1, K. Madhurabhasini2 “Enhancing Security in Wireless Sensor Network Using Load Balanced Data Aggregation Tree Approach”, 2015

[5] Jugminder Kaur, Sandeep S. Gill, and Balwinder S. Dhaliwal "Secure Trust Based Key Management Routing Framework for Wireless Sensor Networks", 2016
[6] Dr. Amit Sharma et al. 2016 "Security and Integrity Aware Deep Learning Based Approach for Wireless Communications", 2016

