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.160 – 168

Trust Based Shortest Path Routing Algorithm to Enhance Security 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 - This paper introduces the security and trust concepts in wireless sensor networks and explains the difference between them, stating that even though both terms are used interchangeably when defining a secure system, they are not the same. Highlighting that reputation partially affects trust. 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 [8].

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.

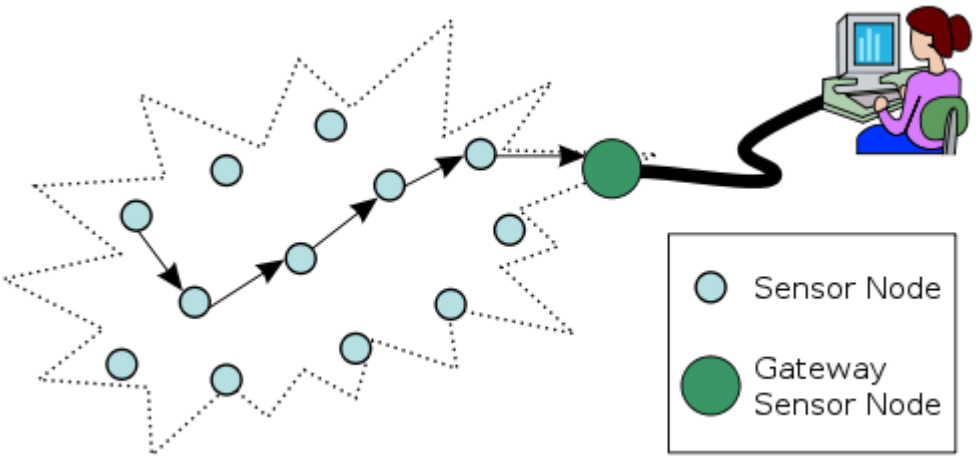

Figure 1 Wireless Sensor Network

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

Previously AODV is developed with 50 nodes in MATLAB [21].

In previous research AODV are performed and the result of previous research is given by

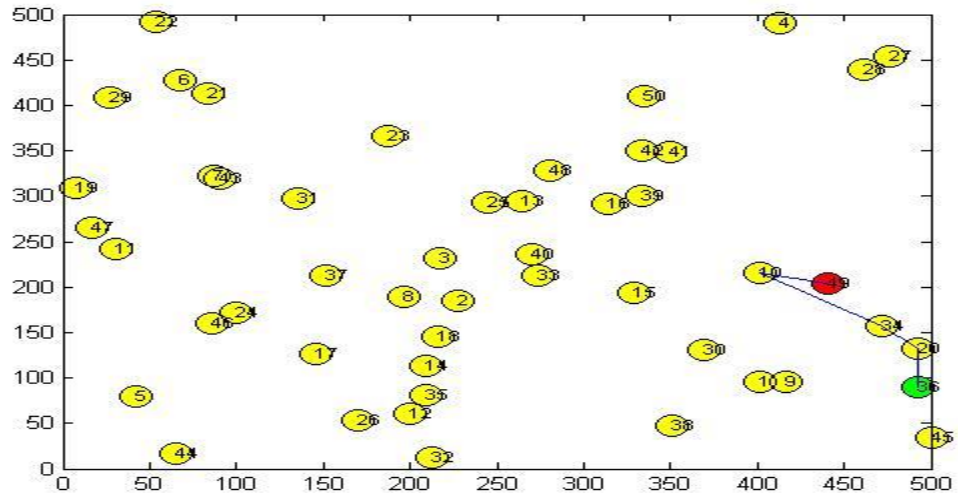

Figure 2 Existing 50 Nodes Scenario

The figure 2 shows the scenarios that consists of 20 nodes, 36 is selected as the destination node and 49 is selected as the source node. The transmission of the data from source to destination is also shown above.

3. Objectives

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 level 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

.For MTR we are using a 500 × 500 network of 70 sensor nodes for simulation using MATLAB. Let 40% nodes be the advanced nodes taking that is more than the previous algorithm nodes

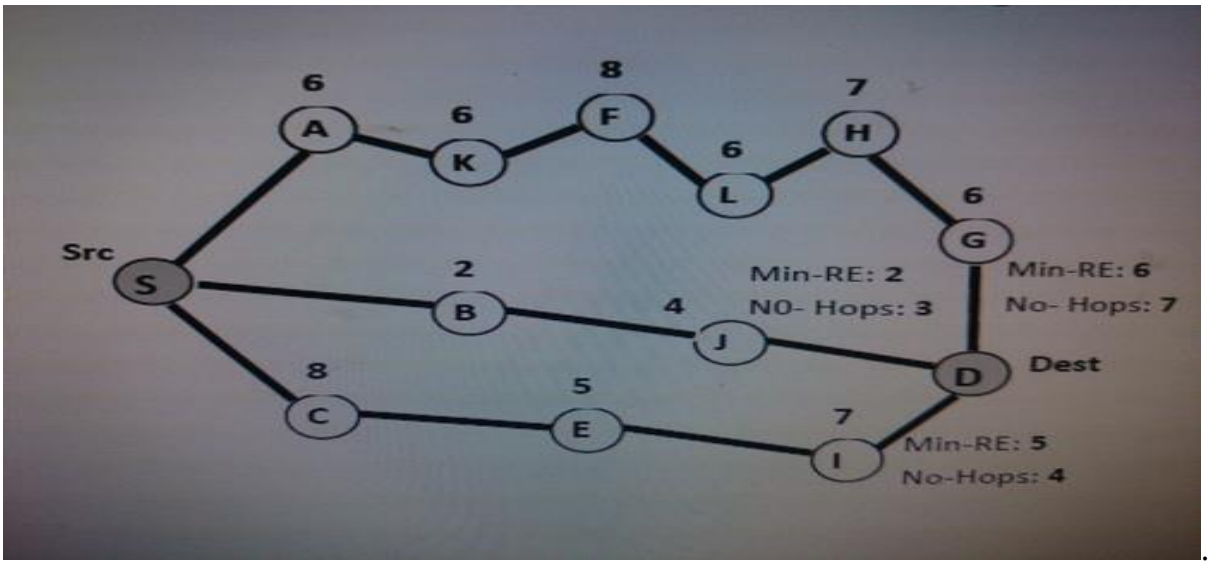

Figure. 2 Evaluation of Minimum shortest path with trust.

Here a simple routing is considered from source node S to destination node D. The number written on a node represents the value of residual node energy. Since the route 1 considers only the minimum hop count, it selects route <S-B-J-D> which has the hop count of 3. In route 2, data is transferred from source to destination node by choosing the route <S-C-E-I-D> which has largest α value of 1.25. Route 1 selects the shortest path without considering residual energy of nodes, which is the same as the MTR routing algorithm. Route 2 improves the drawbacks of Route 1 by considering both residual energy and hop count. It improves the lifetime of network by making almost all nodes to involve in data transfer [8].

5. Results

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.

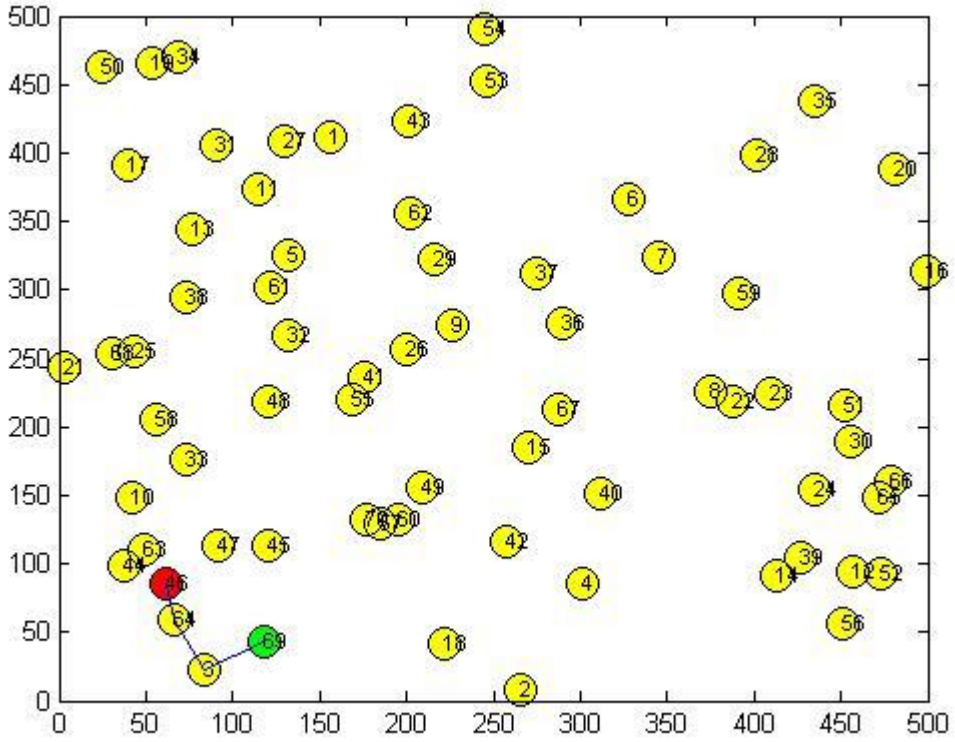

Figure 4.2: Existing 70 Nodes Scenario

The figure 4.2. shows the scenarios that consists of 70 nodes , 69 is selected as the destination node and 46 is selected as the source node. The transmission of the data from source to destination is also shown. This figure show the shortest and secure path as compare to the previous figure.

6. Conclusion

Routing performance namely delivery ratio of MTR is determined and also compared with AODV protocol by varying the malicious nodes from 0 to 20 for 70 nodes with coverage area of 500×500 m^2. The results show that an improvement of approximately 20% in delivery ratio is achieved by using the MTR protocol than the AODV. This is mainly due to the successful transmission of packets from source to destination nodes by considering trusted path along with path having minimum energy level nodes and shortest route.

7. Future Scope

If the number of nodes are increased for finding shortest path and trust value among the nodes then the data is transferred from source to destination improves data delivery ratio and minimum hop count and energy of the nodes. In future, any new criteria is merged with the existing algorithm then also improves the data delivery ratio throughput, minimum hop count and energy of nodes.

References

[1] D. Harrison McKnight and Norman L. Chervany "Trust and Distrust Definitions: One Bite at a Time", 2001

[2] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci "Wireless sensor networks: a survey", 2001

[3] Kemal Akkaya , Mohamed Younis "A survey on routing protocols for wireless sensor networks", 2003

[4] Jaydip Sen "A Survey on Wireless Sensor Network Security", 2009

[5] Ewa Niewiadomska-Szynkiewicz, Piotr Kwaśniewski, and Izabela Windyga "Comparative Study of Wireless Sensor Networks Energy-Efficient Topologies and Power Save Protocols", 2009

[6] T.Kavitha, D.Sridharan "Security Vulnerabilities In Wireless Sensor Networks: A Survey", 2009

[7] EwaNiewiadomska-Szynkiewicz, PiotrKwaśniewski, and IzabelaWindyga "Comparative Study of Wireless Sensor Networks Energy-Efficient Topologies and Power Save Protocols", 2009

[8] Mohammad Momani , SubhashChallaet "Survey of Trust models in Different Network Domain", 2010

[9] Theodore Zahariadis1, Helen C. Leligou, PanagiotisTrakadas and StamatisVoliotis "Trust management in wireless sensor networks", 2010

[10] Mohammad Momani "Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks", 2010

[11] Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago "Trust Management Systems for Wireless Sensor Networks", 2010

[12] Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis,Panagiotis Trakadas, Ioannis Papaefstathiou,Charalambos Vangelatos, Lionel Besson "Design and implementation of a Trust-Aware Routing Protocol for Large WSNs", 2010

[13] PedramRadmand, Alex Talevski, Stig Petersen and Simon Carlsen "Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries", 2010

[14] P.Samundiswary "Trust based Energy aware Reactive Routing Protocol for Wireless Sensor Networks", 2012

[15] Krzysztof Daniluk*a*andEwaNiewiadomska-Szynkiewicz*a "*A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks*"' 2012*

[16] Deepika Thakral Neha Dureja "A Review on Security Issues in Wireless Sensor Networks",2012

[17] Zhongwei Chen et al., "Multivalued trust routing based on topology level for wireless sensor networks", 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.

[18] Chen, Z., Zhang, R. Ju, L., & Wang, W. (2013, July). Multi valued Trust Routing Based on Topology Level for Wireless Sensor Networks. In Trust, Security and Privacy in Computing and Communications (Trust Com), 2013 12th IEEE International Conference on (pp. 1516-1521) IEEE.

[19] Mukesh Kumar Garg, Dr. Ela Kumar, "Routing Issues for Trust Based Framework in Mobile Ad Hoc Networks", 2013

[20] D. Sheela, G. Mahadevan "Mobile Agent Based Enhanced Security for Wireless Sensor Networks", 2014

[21] E. Thenmozhi ,S. Audithan "Trust based cluster and secure routing scheme for wireless sensor network", 2014

[22]Dongxia Wang, Tim Muller, Yang Liu, and Jie Zhang "Towards Robust and Effective Trust Management for Security: A Survey", 2014

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

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

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

[26] Jugminder Kaur, Sandeep S. Gill, and Balwinder S. Dhaliwal "Secure Trust Based Key Management Routing Framework for Wireless Sensor Networks", 2016

[27] Dr. Amit Sharma et al. 2016 "Security and Integrity Aware Deep Learning Based Approach for Wireless Communications", 2016

