
Nagesh Kumar, Jaypee University of Information Technology, Waknaghat, India
Yashwant Singh, Central University of Jammu, Jammu, India
Pradeep Kumar Singh, Department of CSE and IT, Jaypee University of Information Technology, Waknaghat, India

ABSTRACT

As the wireless sensor networks (WSN) are gaining popularity the need of reliable delivery of data packets becomes more important. The reliable delivery is only possible when the routing protocols are efficient and secure. Because of lack of resources it is not possible to use existing cryptosystems to provide security in WSN. But, trust aware routing can provide the security with lesser resources, which become popular in last three to four years. In this paper, a new energy efficient and trust aware reliable opportunistic routing (TAEROR) protocol is proposed. The protocol consists of a trust metric and also a relay selection algorithm. The trust aware metric detects the malicious nodes on the basis of forwarding sincerity, energy consumption and acknowledgement sincerity. Relay selection algorithms avoid these malicious nodes to get selected in the routing process. The protocol is simulated and compared to existing trust aware routing protocols. Proposed protocol TEAROR presents better results than the other compared protocols.

KEYWORDS

Energy Efficiency, Opportunistic Routing, Sensor, Trust, WSN

1. INTRODUCTION

In most of the applications of Wireless Sensor Networks (WSN), the sensor nodes are operating independently without any external interference. This unsupervised operation of WSN leads to expose nodes to variety of malicious attacks. There are many protocols (Haque et al., 2008) (Hu et al., 2003) (Zhang et al., 2008) (Mohaisen et al., 2009) (Ahmed et al., 2016) developed, most of which are based on cryptographic and authentication systems. These algorithms/protocols are not successful for wireless sensor networks for the following reasons:

1. These protocols are mostly based on the assumption that all nodes in the network are helpful and truthful during the routing process. This assumption makes the protocols unrealistic especially for insider attacks (Slehi et al., 2016);

DOI: 10.4018/IJISMD.2017040102

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
2. The sensor nodes are having limited resources like battery power, storage capacity and processing capacity. These constraints restrict the use of the most of cryptographic algorithms. Because cryptosystems need to be executed with high processing, storage and power consumption (Ahmed et al., 2016);

3. In cryptographic and authentication systems there is requirement of centralized key management agent which is not possible to install in WSN.

For the purpose of security of data packets and routing processes in WSN trust and reputation based systems were proved to be more efficient against node mischievousness occurrences. Trust and reputation aware methods are new to solve the problem of security without using cryptosystems (Cordasco and Wetzel, 2008). The trust of a node in wireless communication networks can be defined as the “…degree of reliability of neighbor nodes performing routing process (sending and receiving packets) …” (Govindan and Mohapatra, 2012). These methods help the sensor nodes in making decisions about other nodes to select them as next-hop forwarders, in other words trust and reputation based routing methods predict the future behavior of neighbor nodes. As the WSN are opportunistic networks in nature, hence, trust and reputation based security systems are more suitable. In opportunistic networks every node on the routing path have the opportunity of send data toward the destination and no fixed path is followed. Hence, trust and reputation based methods helps the opportunistic routing processes to decide the best next-hop forwarder. Trust based methods in WSN are similar to the human behavior system, where two nodes will communicate to each other only when the trust level of receiving node is up to the mark at a certain period of time. The trust values of sensor nodes in WSN should be updated after a certain period of time for the purpose of maintaining low risk level. As the trust based routing protocols do not involve the malicious and misbehaving nodes into the routing process, the throughput and energy efficiency of the network will be improved automatically.

Working on trust and reputation based methods in recent years many protocols have been proposed (Srinivasan et al., 2006) (Ganeriwal et al., 2008) (Michiardi and Molva 2002) (Zaharia et al., 2013) (Tanachaiwiwat et al., 2004) (Gheorghe et al., 2013) (Choudhary et al., 2008) (Channa and Ahmed, 2011). However, most of the protocols have fixed path routing processes. In WSN the fixed path routing processes introduce delays and also if any node on the fixed path is dead, then routing processes are needed to rebuild it. Also, existing trust and reputation based approaches have many vulnerabilities. For example, most of the trusted nodes, in a trust based routing protocol, are the neighbor nodes which are having low energy. This will lead to a short network lifetime. There are several number of packets flow in the network at the same time, which increase the overhead of routing processes. Also, most of the trusted protocols are designed for MANETS and executed on strong hardware platforms having good resources. There is a need of dynamic trust based routing processes to detect the malicious behaviors in the network.

Opportunistic routing provides the ability to sensor nodes to utilize the broadcasting capabilities in a better way. Although there is a risk to data and routing process because of broadcasting, because when the node broadcast a packet it can also be received by malicious nodes. The malicious nodes can misuse these packets to destroy network or to spread false information. The motivation is to provide security to these packets as well as enhance the network lifetime by reducing the energy consumption. The trust aware protocols provide this facility with less energy consumption. The trusted nodes will be included in the routing process and the malicious or untrusted nodes will be avoided.

This paper announces a new trust based and reliable opportunistic routing protocol for WSN. The protocol has been designed to overcome the limitations of existing trust based routing schemes
Related Content

Choosing Basic Architectural Alternatives
[www.igi-global.com/chapter/choosing-basic-architectural-alternatives/8237?camid=4v1a](www.igi-global.com/chapter/choosing-basic-architectural-alternatives/8237?camid=4v1a)

Metamorphic Relations Based Test Oracles for Image Processing Applications
[www.igi-global.com/article/metamorphic-relations-based-test-oracles-for-image-processing-applications/144139?camid=4v1a](www.igi-global.com/article/metamorphic-relations-based-test-oracles-for-image-processing-applications/144139?camid=4v1a)
Security Testing Framework for Web Applications
*International Journal of Software Innovation* (pp. 93-117).
www.igi-global.com/article/security-testing-framework-for-web-applications/207728?camid=4v1a

Retrofitting Existing Web Applications with Effective Dynamic Protection Against SQL Injection Attacks
www.igi-global.com/article/retrofitting-existing-web-applications-effective/39007?camid=4v1a