ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

PERFORMANCE AND IMPACT ANALYSIS OF SPIN PROTOCOL UNDER SYBIL ATTACK

Rohit Choudhary*, Er. Amanpreet Kaur, Prashant Maurya
* Research Scholar Centre Of CST Central University of Punjab Bathinda, India
Assistant Professor Centre Of CST Central University of Punjab Bathinda, India
Research Scholar Centre Of CST Central University of Punjab Bathinda, India

ABSTRACT

Wireless sensor network is an emerging field of research and has attracted a lot of researchers because of its applicability in remote and hostile environments. Since wireless sensor networks communicate over an open wireless medium on specified radio frequencies, they are prone to interference as well as attacks. The intent of our study is to investigate the security of SPIN (Sensor protocol for Information via negotiation) protocol under active routing attack called Sybil attack. This paper summarizes the performance of SPIN under ideal conditions and under Sybil attack.

KEYWORDS: SPIN, Security, Sybil attack.

INTRODUCTION

Wireless sensor networks consist of hundreds of low power, low cost sensor nodes which communicates over wireless medium using radio frequencies.

When sensor nodes are deployed in large number in an open medium they are susceptible to attack. An attacker may capture and reprogram the nodes. They may use their own developed algorithms to accept them as legitimate nodes in the network[1]. The adversary can perform modification of data packets, dropping of packets, injection of false packets or other actions which a node is not expected to perform in a routing protocol[2].

Literature study indicates that SPIN has not been checked for Sybil attack. It is necessary to check the performance of any protocol under attack as it provides a base to enhance that protocol. This paper aims to evaluate the performance of data centric protocol namely SPIN (Sensor protocol for Information via Negotiation) Protocol under active attack called Sybil attack which poses a serious threat to routing algorithm's performance and security in wireless sensor network.

SECURITY REQUIREMENTS

To provide security in the network there must be some security requirements that should be achieved. The some of the security requirements are listed below [1][3].

- **Authentication**: It ensures that an illegitimate node cannot capture any node in the network.
- **Confidentiality**: It is the ability to hide message from an illegitimate user i.e. the user outside the network does not understand the message.
- **Integrity**: It provides the surety that the message sent from sender to receiver has not been tampered with.
- **Availability**: It ensures that the network services up whenever a nodes prompts a requests for communication in the network.
- **Non repudiation**: It ensures that nodes in the network cannot deny the message it has previously sent.

So in order to build a secure sensor network one must ensure that these security requirements are met

SPIN PROTOCOL

SPIN is a negotiation based protocol used to efficiently disseminate information in a wireless sensor network. Earlier data dissemination approaches like flooding and gossiping wastes the energy resources by sending duplicate information throughout the network. Moreover, these protocols were not resource-adaptive. SPIN solved these shortcomings of conventional approaches by data negotiation and resource-adaptive algorithms. SPIN assign a high-level name to their data, called meta-data, and perform meta-data negotiations before any data is transmitted. This assures that there is no redundant data sent throughout the network. In addition, SPIN has access to the current energy level of the node and adapts the protocol based upon remaining energy [4].

The SPIN family of protocols are based on two basic assumptions:

- First, before sending the actual data the nodes exchange the meta-data to negotiate with neighbours and hence conserve the energy by operating more efficiently.
- Secondly in conventional flooding and gossiping-based routing protocols the energy and bandwidth of the network is wasted by sending unnecessary copies of data in overlapping areas.

SYBIL ATTACK

In Sybil attack a single node A presents multiple identities to other nodes in the network by pretending to be legitimate node or by claiming false identities as shown in figure1. The Sybil attack can reduce the effectiveness of fault-tolerant schemes such as multipath routing and topology maintenance in SPIN protocol.

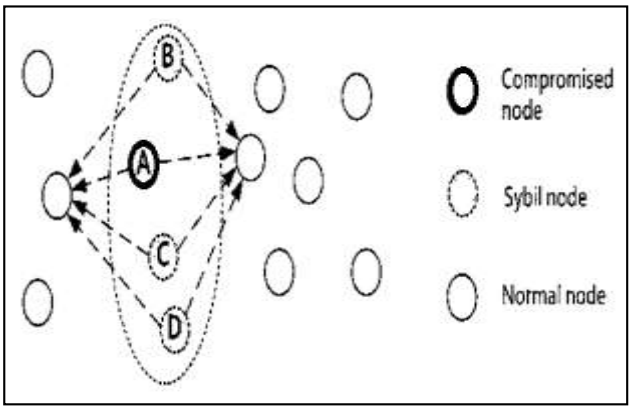

Figure 1. Sybil Attack

In data aggregation a single Sybil node may able to aggregate several data readings as many times as it shows its identity in the network. With large number of Sybil nodes in the network an attacker may alter several aggregated readings [5].

SIMULATION TOOL

To validate the correctness and do the performance test of SPIN protocol NS 2.34 is used for simulation.

NS2 is a discrete event simulator aimed at networking research. NS2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks[6].

NS2 is object oriented simulator written in C++ (front-end), with an Otcl interpreter at front-end. NS 2 supports variety of protocols, traffic models etc .The various features of NS2 are listed below

- Protocols: TCP, UDP, HTTP, Routing algorithms.
- Traffic Models: CBR, VBR, Web etc.
- Error Models: Uniform, Bursty etc
- Radio Propagation, Mobility models
- Energy Models
- Topology Generation tools
- Visualisation tools

PERFORMANCE METRICS

The performance metrics to evaluate the performance of the SPIN routing algorithm are listed below;

A. *Throughput:* It is the average rate of successful message delivery over the network. It is measured in KBPS.
B. *Average Delay:* It is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue (waiting time) in data packet transmission.
C. *Packet Delivery Ratio*: The ratio of the number of data packets delivered to the destination to the total number of packets sent by the source node. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol. It is measured in % ratio.
D. *Energy Spent*: It is the average energy spent by the nodes for communication in the network. It is measured in Joules.

RESULTS AND DISCUSSIONS

This section discusses section the results obtained after simulating the wireless sensor networks using SPIN protocol. The network performance is measured using performance metrics given in section VI.

The values for the results are taken using AWK scripts in NS 2.34.

A topology of wireless sensor networks with 50 nodes is created, transmission of packets between the nodes is done using SPIN protocol with CBR traffic with few nodes programmed as Sybil nodes in the network.

Throughput

The throughput of SPIN protocol has degraded in the presence of Sybil attack. Figure 2 shows that the rate of delivery of the packets in the network has degraded because the Sybil nodes does not forward the packets instead it aggregates them and eventually drops them.

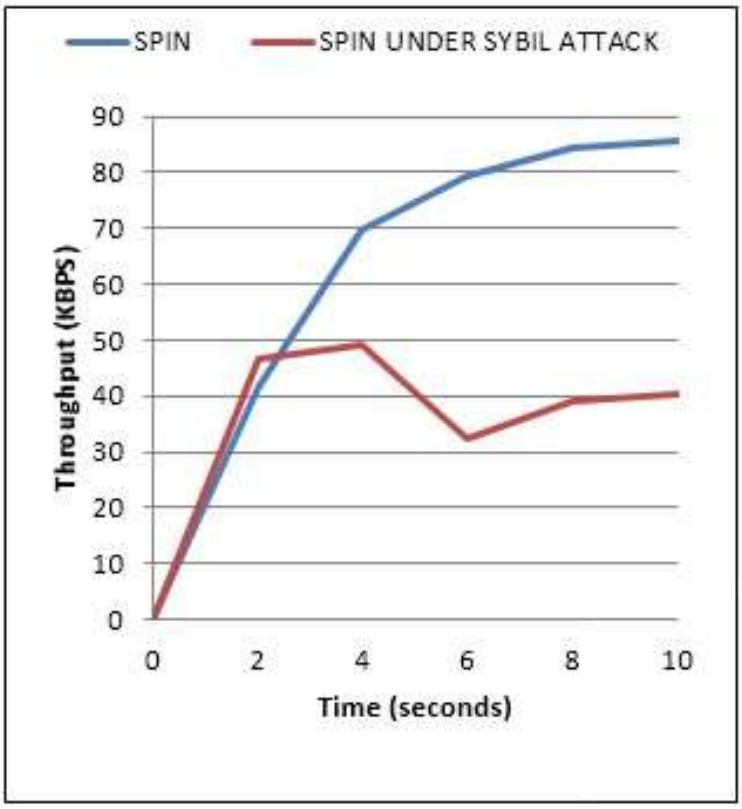

Figure 2. Throughput

Average Delay

The average delay of SPIN protocol under Sybil has also increased as Sybil keep on aggregating the data and drops them. The nodes interested in data keeps on sending the request messages as a result network's average delay increases. The average delay is shown in fig 3.

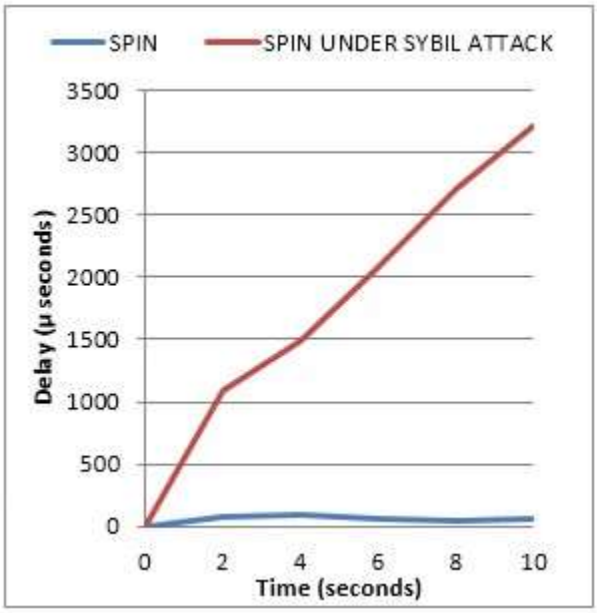

Figure 3. Average Delay

Packet Delivery Ratio

The Figure 4 shows that packet delivery ratio (Pdr) has decreased by significant amount in the network under Sybil attack.

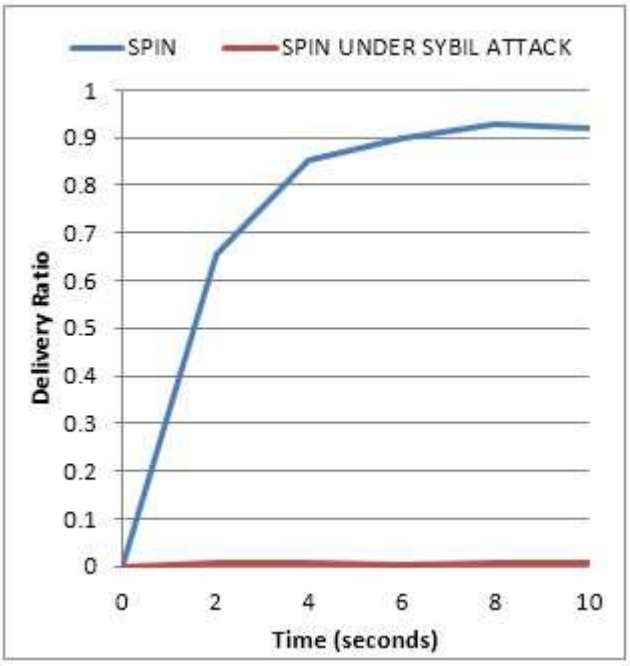

Figure 4. Packet delivery ratio

Energy Spent

The energy spent in the presence under Sybil attack has also increased for SPIN protocol as shown in figure 5.

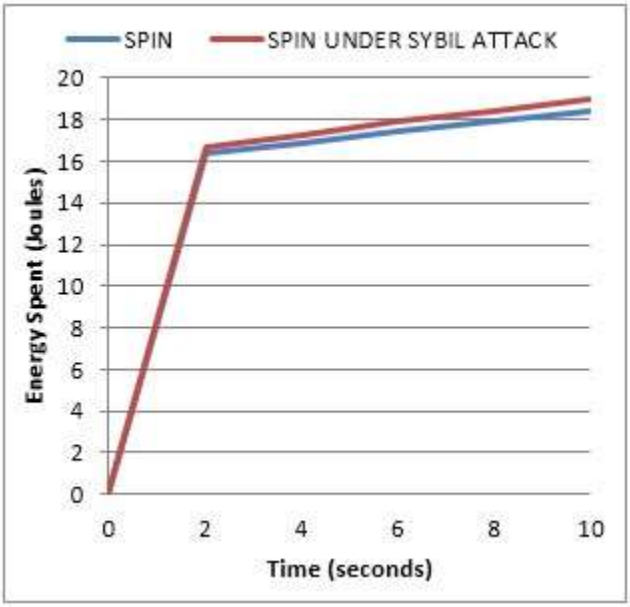

Figure 5. Energy Spent

CONCLUSION & FUTURE WORK

In this study when SPIN protocol is exposed to Sybil attack in which a node maliciously presents its multiple identities to aggregate data, performance of the network degrades drastically.It is also notable that Sybil attack poses serious threat to the network where the security of network is main concern. As the Sybil nodes are able to intrude and temper the sensed data in the network which is evident from the results obtained in section VII.

It has also been concluded that SPIN protocol in its normal operation gives much better performance of the network and data is disseminated at appropriate level (almost 90% of data is disseminated) in whole of the network. So the SPIN protocol adheres to its principle of data dissemination.

In future we suggest there is a need to integrate a security mechanism which must ensure the security for SPIN protocol by authenticating the nodes in the network. We also suggest that a new enhanced scheme should be developed with cryptographic techniques. The enhanced scheme should provide a authentication and confidentiality to ADV and DATA packets in the network. So that security requirements for the network are met.

REFERENCES

[[1]Y.-X. Li, L. Qin, and Q. Liang, "Research on wireless sensor network security." pp. 493-496.
[2]L. Tang, and Q. Li, "S-SPIN: A provably secure routing protocol for wireless sensor networks." pp. 620-624.
[3]A. Modirkhazeni, N. Ithnin, and O. Ibrahim, "Secure multipath routing protocols in wireless sensor networks: a security survey analysis." pp. 228-233.
[4]W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks." p. 10 pp. vol. 2.
[5]J. Newsome, E. Shi, D. Song et al., "The sybil attack in sensor networks: analysis & defenses." pp. 259-268.
[6]"The Network Simulator - ns-2," 21 January, 2013; http://www.isi.edu/nsnam/ns/