International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 6, No 4, 2018, pp 01-06
https://doi.org/10.18510/ijsrtm.2018.625

A SOLUTION TO SELECTIVE FORWARD ATTACK IN WIRELESS SENSOR NETWORK

Gulbir Singh[1*], Dr. Om Prakash Dubey[2], Gautam kumar[3]
[1,3]Assistant Professor, MMICT&BM, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana—133207 (India), [2]Veer Kunwar Singh University, Ara, Bihar – 802301 (India).
Email: [*]gulbir.rkgit@gmail.com

Article History: Submitted on 15th August 2018, Revised on 28th September 2018, Published on 03rd October 2018

Abstract

Purpose of Study: Wireless mesh network represents a solution to provide wireless connectivity. There are some attacks on wireless sensor networks like black hole attack, sinkhole attack, Sybil attack, selective forwarding, etc. In this paper, we will concentrate on a selective forwarding attack. Selective Forwarding Attack is one of the many security threats in wireless sensor networks that can degrade network performance. An adversary on the transmission path selectively drops the packet. The adversary same time transfers the packet, while on a few occasions it drops the packet. It is difficult to detect this type of attack since the packet loss may be due to unreliable wireless communication. The proposed scheme is based on the trust value of each node. During data transmission, a node selects a downstream node that has the highest trust value, which is updated dynamically based on the number of packets a node has forwarded and dropped.

Methodology: A comparative methodology is used in all existing schemes. We compared our scheme with the existing scheme and found that the packet loss in the proposed scheme is much less than the existing scheme.

Result: We showed that our scheme essentially detects malicious nodes for each possible scenario. Regarding communication overhead, our scheme is more efficient than typical multipath schemes. Also, by utilizing an existing routing protocol which is secure against sinkhole attacks, our scheme also provides security against sinkhole attacks.

Keywords: *Wireless mesh network, AODV, Routing, Selective Forward Attack, NS-2, ADHOC Networks.*

INTRODUCTION

WMNs are not built on a fixed infrastructure. Instead of this, hosts rely on each other to keep the connection. WMNs provide low-cost broadband internet access, wireless LAN coverage and network connection to fixed or mobile hosts for both network operators and users. The reason for preferring WMNs is easy, fast and deployment of the technology. A WMN consists of mesh routers and mesh clients. Mesh routers are fixed. They have a wireless infrastructure and work with the other networks to provide a multi-hop internet access service for mesh clients. On the other hand, mesh clients can connect to the network over both mesh routers and other clients. In these networks, due to a large number of nodes, working through some issues like security, scalability, and manageability is required. Thus, new applications of WMNs make secrecy, and security mechanisms are necessities each sensor node consists of a radio transceiver for communication purposes, a microcontroller for processing abilities, a sensor for sensing or monitoring and battery for providing energy. Some of the popular applications of the sensor network are area monitoring, environment monitoring (such as pollution monitoring), industrial and machine health monitoring, wastewater monitoring and military surveillance. Security is crucial for wireless sensor networks deployed in hostile environments. Providing security solutions to these networks is difficult due to its characteristics such as tiny in nature and constraints in resources. One of the attacks in WSN is the Selective Forwarding attack.

LITERATURE SURVEY AND RELATED WORK

A. Detection using Watermark in Wireless Sensor Networks

CIanF. Akyildiz, XudongWang, Weilin Wang (2010): In this paper to proposed a scheme of secure data transmission which can forward the data safely, and detect the selective forwarding attack judge the trust value of each node to select a secure path for message forwarding and then use the watermark technology to detect the malicious nodes which are suspected to launch selective forwarding attack. When such an attack is detected, the detection mode starts. The malicious node can be detected and addressed. The watermarking technique is used to protect data transmission safely.

Singh, G., Dubey, D. O. P., & Dey, M. (2017) carried out the comparison of Geographical and Topological Multicast Routing Protocols on WSN using NS-2 Simulator.

B. CHEMAS

This paper is presented by A. Boukerche (2013) proposed performance evaluation of routing protocols for ad hoc wireless networks.

A multi-hop acknowledgment scheme for detecting selective forwarding attacks. The intermediate nodes are responsible for detecting the misbehavior of the nodes.

C. **A Polynomial-based Countermeasure to Selective Forwarding Attacks in Sensor Networks**

YS.R. Das, C. E. Perkins and E. M. Royer (2011) have proposed a polynomial modeling based countermeasure against selective forwarding attack and a security scheme using redundant data to tolerate the loss of critical event messages. The basic idea is to split the sensing data into parts and to send these parts instead of the original sensing data to the sink by adopting a dynamic individual path forwarding mechanism so that, the forwarding nodes cannot understand the contents of the data generated by the polynomial, which can prevent eavesdropping.

D. **Security Issues in Wireless Sensor Networks**

Gautam U, Singh G (2014), provides a comparative study of TCP protocol over Network Routing Protocols for Mobile Ad Hoc Networks. Given this paper provides an overview of security issues known so far in wireless sensor networks. In the absence of adequate security, deployment of sensor networks is vulnerable to a variety of attacks. In this paper, we have discussed threat models and unique security issues faced by wireless sensor networks.

E. **Intrusion Detection for Routing Attacks in Sensor Networks**

Singh G (2014), implemented a comparative study of three routing protocols(DSDV, AOMDV, DSR) in MANETS using Network Simulator 2. We present a method for intrusion detection in wireless sensor networks. Our intrusion detection scheme uses a clustering algorithm to build a model of normal traffic behavior and then uses this model of normal traffic to detect abnormal traffic patterns.

F. **CADE**

Cumulative Acknowledgement based Detection Selective Forwarding Attacks in Wireless Sensor Networks By A. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, M. Turon (2006). This present a detecting scheme which identifies malicious nodes delivering selective forwarding attacks without the need for time synchronization

PROPOSED APPROACH

A. Main Idea

Security is a recent topic in the Routing protocol in recent days. The main issue is how we secure our communication? Many papers publish in this area some purposed Hash functions for hop count, some use the Hash chain for Sequence no. **Detection using a multihop acknowledgment scheme:** A Distributed detection scheme that uses multi-hop acknowledgments from intermediate nodes to raise alarms in the network. This scheme focuses on a selective forwarding attack in which detection occurs in both the base station and source nodes. In this scheme, each intermediate node along the forwarding path is in charge of detecting malicious nodes. If an intermediate node detects the misbehavior of its downstream (upstream) nodes, it will generate an alarm packet and deliver it to the source node (the base station) through multiple hops. The base station and the source node can then use more complicated IDS (Intrusion Detection System) algorithms to make decisions and responses. The authors have used routing and transport protocols such as Directed Diffusion

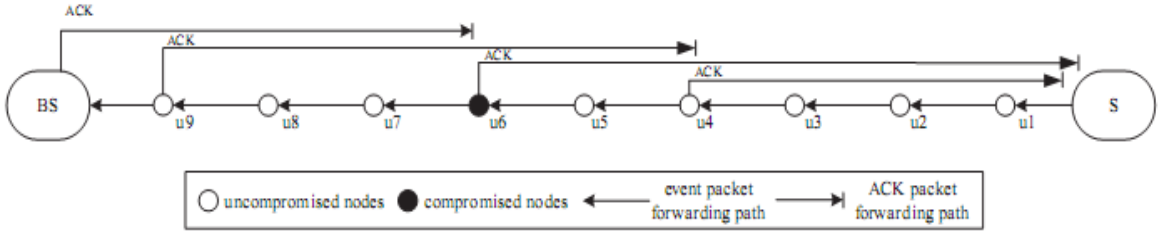


Figure 1: An example of multihop acknowledgment. Node u4, u6, u9 are selected as a checkpoint

CHEMAS: Identify suspect nodes in selective forwarding attacks. A technique for identifying suspect nodes in a selective forwarding attack. The technique for the detection of a selective forwarding attack is named CHEMAS (checkpoint-based multi-hop acknowledgment scheme). This scheme randomly selects part of intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgments for each packet received. Also, the node needs a one-way hash key chain for ensuring the authenticity of packets. Delay mechanisms are also developed to

send the current one-way hash key. Each intermediate node in a forwarding path has the potential to detect abnormal packet loss and identify suspect nodes if it does not receive enough acknowledgments from the downstream checkpoint nodes.

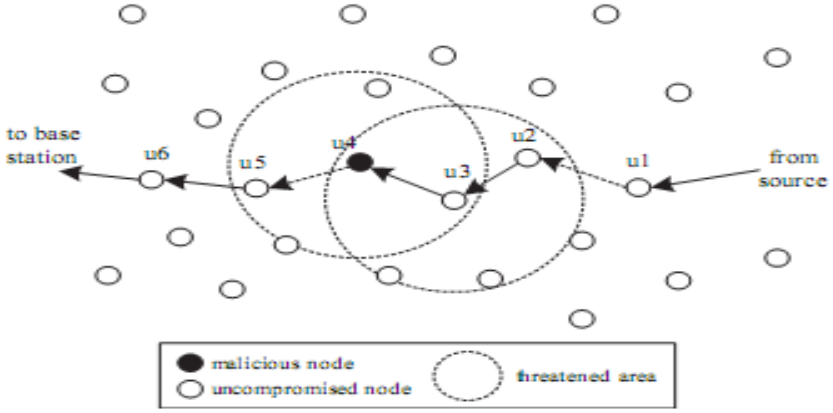


Figure 2: Identification of suspect node

Detecting Selective Forwarding Attacks in Wireless Sensor Networks using SVMs

A centralized intrusion detection scheme based on Support Vector Machines (SVMs) and has used sliding windows for black hole attacks and selective forwarding attacks. In this scheme, they only detect the attacks. This scheme uses routing information local to the base station of the network and raises alarms based on the 2D feature vector (bandwidth, hop count). Classification of the data patterns is performed using a one-class SVM classifier. They use anomaly detection as a base for their scheme. Anomaly detection signals an intrusion when the observed activities differ significantly from those usually undertaken by the user.

Fuzzy-Based Reliable Data Delivery for countering selective Forwarding in Sensor Networks

A Fuzzy-based reliable data delivery scheme for countering selective forwarding attack which is an improved form of Multi-path routing method. The enhancement is that the number of transmission path varies with a number of the attacker.

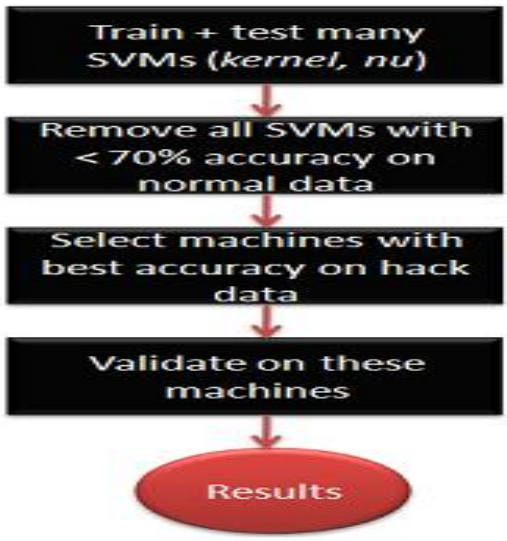


Figure 3: SVM Selection Process

Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks

A distributed lightweight defense scheme against a selective forwarding attack, which is based on a hexagonal WSN mesh topology. This scheme utilizes the neighbor nodes to monitor the transmissions of the event packet and detect selective

forwarding attack by monitoring packets' forwarding of two nodes in the transmission path, and resend these packets dropped by the attackers to the destination node.

Proposed Prevention Technique

We proposed an efficient defensive scheme against a selective forwarding attack. In our scheme, nodes monitor their neighbor nodes and if they act as malicious then broadcasts an alert packet. Our scheme relies on the broadcast nature of sensor networks. Instead of discarding the packets, the node monitors whether the destination is forwarding the packet or not.

RESULT AND IMPLEMENTATION

A. NS2 Network Simulator

We use the NS2 tool (NS2.34 Version) for our implementation on Linux 14.04 Operating System. Before going on the Result, we take a short view of NS2. NS is a simulator program work on the network as event-driven, developed at California University Barkley, which has many network objects like applications, traffic source behavior, and protocols.

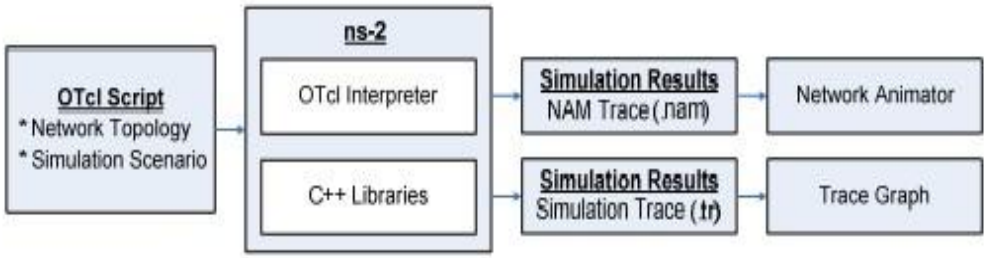
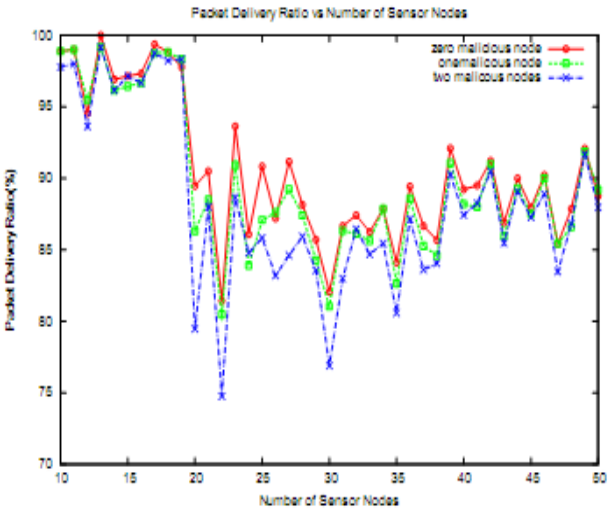


Figure 4: Working process of NS-2 simulator

B. Packet delivery ratio

It is observed from Figures 4, 5, 6, 7 that the packet delivery ratio in the presence of malicious node is higher on the proposed scheme. This is because in the proposed scheme a node selects a trusted downstream to deliver a packet to the sink node. In case of a packet loss, it retransmits to the next most trusted download link.



International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 6, No 4, 2018, pp 01-06
https://doi.org/10.18510/ijsrtm.2018.625

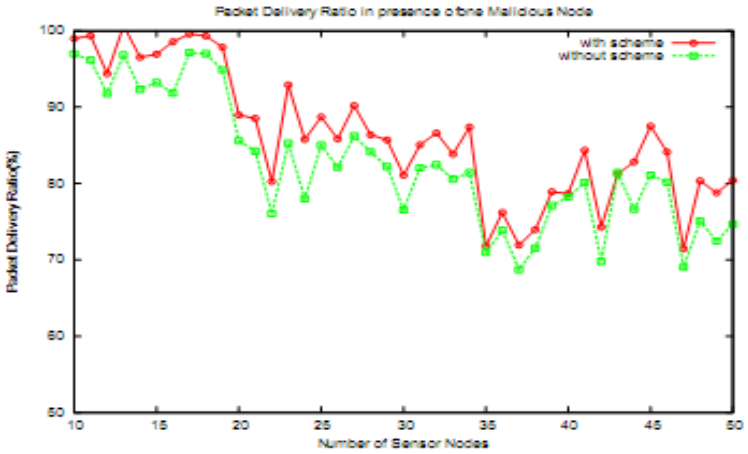


Figure 5: Packet Delivery Ratio vs. Number of Sensor Nodes in the presence of one Malicious Node

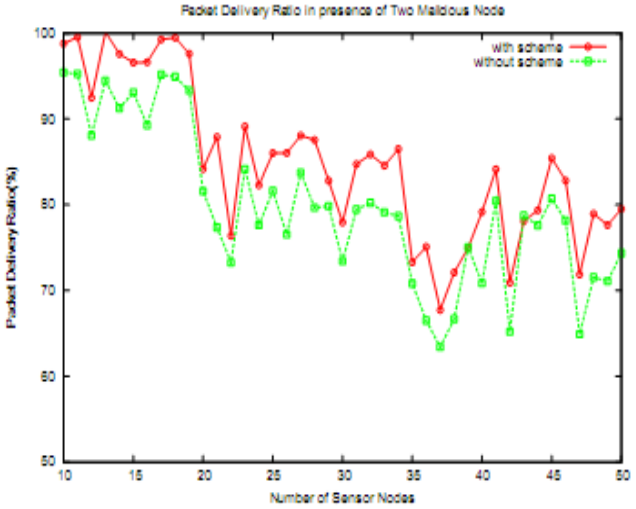


Figure 6: Packet Delivery Ratio vs. Number of Sensor Nodes in the presence of two Malicious Node

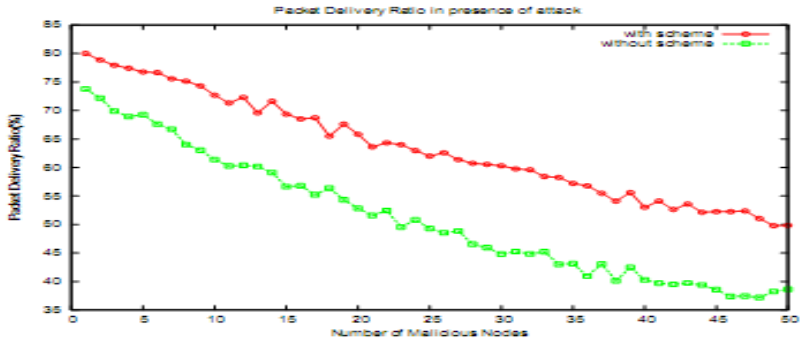


Figure 7: Packet Delivery Ratio vs. Number of Malicious Node for a network of 100 nodes

CONCLUSION

For data transmission, we use the multi-hop system. In the multi-hop system from which route, we transmission our data is an issue. For selecting route among multi-hop and multiple paths, known as Routing. Routing security is an important issue in WMN as well as another wireless network. We need to consider a better tradeoff between higher security and network

performance while designing a secure protocol for routing. Selective forwarding attacks can be serious threats on wireless sensor networks. In this paper, we presented an efficient detection scheme against selective forwarding attacks. We showed that our scheme essentially detects malicious nodes for each possible scenario. Regarding communication overhead, our scheme is more efficient than typical multipath schemes. Also, by utilizing an existing routing protocol which is secure against sinkhole attacks, our scheme also provides security against sinkhole attacks. To reduce the communication overhead as well as to save the consuming energy in each sensor node, we can deliver packets normally in a leisure period, only activating the detection scheme in some sensitive intervals. Several potential approaches remain to be taken to improve the defense capabilities of our scheme. For instance, the use of downstream detection would help the base station to collect alert information; the incorporation of proper redundancy.

REFERENCES

1. A. Boukerche (2013). Performance evaluation of routing protocols for ad hoc wireless networks. *Mobile Networks and Applications, Vol.9, No.4, pp.333-342.* https://doi.org/10.1023/B:MONE.0000031592.23792.1c
2. A. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, M. Turon (2006). The routing protocol in wireless mesh network: challenges and design considerations. *In Proc. Springer Science LLC. pp. 285-303.*
3. CIanF. Akyildiz, XudongWang, Weilin Wang (2010). Wireless Mesh Network: A Survey, *1-5, 28-29 Dec. 2010*
4. Gautam U, Singh, G (2014). A Comparison of TCP Performance over Routing Protocols for Mobile Ad Hoc Networks. *International Journal of Advanced Research in Computer Science & Technology, Vol2 Issue 2, Ver 2, pg-436-442.*
5. H.M. Nyo and P. Viriyaphol, "Detecting and Eliminating Black Hole in AODV Routing", IEEE, Jan 2011,pp.1-4
6. Singh G (2014). Study of performance of routing protocols for mobile ad-hoc networking in ns-2. *IJAICT, Vol 1, Issue 3, pg 299-306.*
7. Singh, G., Dubey, D. O. P., & Dey, M. (2017). Using an ns-2 comparison of geographical and topological multicast routing protocols on wireless ad hoc networks. *International Journal of Students' Research in Technology & Management, 5*(4), 01-07. https://doi.org/10.18510/ijsrtm.2017.541
8. Wu]V. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proc. IEEE INFOCOM 11, Kobe, Japan (2011).
9. YS.R. Das, C. E. Perkins and E. M. Royer (2011). Performance comparison of two on-demand routing protocols for ad hoc networks. *In Proceedings of the IEEE Conference on Computer Communications (INFOCOM)", Tel Aviv, Israel, pp.312.*

