Selective Forwarding Attack in Wireless Sensor Networks

Preeti Yadav
PG Scholar
Department of Computer Science and Engineering
RPS Group of Institutions,Mohindergarh, Haryana (India)

Megha Yadav
Assistant Professor
Department of Computer Science and Engineering
RPS Group of Institutions,Mohindergarh, Haryana (India)

Abstract

Wireless mesh network represent a solution to provide wireless connectivity. There are number of assaults on remote sensor systems like dark gap attack, sink gapa attack, Sybil attack, selective sending and so on. In this paper we will focus on particular sending assault. Particular Forwarding Attack is one among the numerous security dangers in remote sensor systems which can debase arrange execution. A foe on the transmission way specifically drop parcel. The enemy same time exchange the bundle, while in few events it drops the parcel. It is difficult to recognize this kind of assault since the bundle misfortune might be because of inconsistent remote correspondence. The proposed plan depends on trust estimation of every hub. Amid information transmission a hub chooses a downstream hub that has most astounding trust esteem, which is refreshed progressively in light of the quantity of bundles a hub has sent and dropped. We contrasted our plan and existing plan and found that the bundle misfortune in the proposed plan is a great deal not as much as the current plan.

Keywords- Wireless Mesh Network, AODV, Routing

I. BACKGROUND

A. Introduction

[1].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 of preferring WMNs is easy, fast and deployment of the technology [2 A WMN comprises of work switches and work customers [3]. Work switches are settled. They have a remote foundation and work with alternate systems to give a multi-bounce web get to benefit for work customers. Then again, work customers can interface with system over both work switches and different customers. In these systems, because of substantial number of hubs, working through a few issues like security, adaptability and reasonability is required. In this manner, new uses of WMNs make mystery and security instruments are necessities [4].each sensor hub comprises of a radio transceiver for correspondence reason, smaller scale controller for preparing capacities, a sensor for detecting or observing and battery for giving vitality. A portion of the mainstream utilizations of sensor system are territory observing, condition monitoring(such as contamination checking), modern and machine wellbeing observing, squander water observing and military surveillance.[5].Security is vital for remote sensor systems sent in unfriendly situations. Giving security answers for these systems is difficult because of its characteristics, for example, modest in nature and limitations in assets. One of the assaults in WSN, is Selective Forwarding assault.

II. LITERATURE SURVEY AND RELATED WORK

A. Detection using Watermark in Wireless Sensor Networks

Huijuan Deng, Xingming Sun, Baowei Wang, Yuanfu Cao 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, detection mode starts. The malicious node can be detected and addressed. Watermark technique is used to protect the data transmission safely.

B. Chemas

This paper is presented by B. Xiao, B. Yu and C. Gao [4proposed a multi jump affirmation plot for recognizing particular sending assaults. The between intervene hubs are in charge of recognizing the trouble making of the hubs.

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

Xie Lei et al [14] have proposed a polynomial demonstrating based countermeasure against specific sending assault and a security plot utilizing excess information to endure the loss of basic occasion messages. The essential thought is to part the detecting

information into parts and to send these parts rather than the first detecting information to the sink by embracing a dynamic individual way sending component so that , the sending hubs cannot comprehend the substance of the information created by the polynomial, which can forestall listening stealthily.

D. Security Issues in Wireless Sensor Networks

Tanveer Zia and Albert Zomayahas given this paper which provides an overview of security issues known so far in wireless sensor networks. Without satisfactory security, deployment of sensor systems is powerless against assortment of assaults. In this paper we have talked about risk models and extraordinary security issues confronted by remote sensor systems.

E. Intrusion Detection for Routing Attacks in Sensor Networks

By Chong Eik Loo, Mun Yong Ng, Christopher Leckie, MarimuthuPalaniswami. We display a strategy for interruption recognition in remote sensor systems. Our interruption location plot utilizes a bunching calculation to fabricate a model of ordinary movement conduct, and after that uses this model of typical activity to recognize strange movement designs.

F. CADE:Cumulative Acknowledgement based Detection Selective Forwarding Attacks in Wireless Sensor Networks

By Young Ki Kim, Hwaseong Lee, Kwantae Cho, and Dong HoonLee. His display a recognizing plan which identifies malevolent hubs conveying particular sending assaults without the requirement for time synchronization.

III. PROPOSED APPROACH

A. Main Idea

Security is a recent topic in Routing protocol recent days. The main issue is that how we secure our communication? Many papers publish in this area some purposed Hash functions for hop count, some use Hash chain for Sequence no. Detection using multihop acknowledgement scheme: A Distributed recognition conspire that utilizations multi bounce affirmations from transitional hubs to bring cautions up in the system. This plan concentrates on specific sending assault in which location happens in both the base station and source hubs. In this plan, each middle of the road hub along the sending way is accountable for recognizing noxious hubs. On the off chance that a moderate hub recognizes the misconduct of its downstream (upstream) hubs, it will create a caution parcel and convey it to the source hub (the base station) through different bounces. The base station and the source hub can then utilize more confounded IDS (Intrusion Detection System) calculations to settle on choices and reactions. The creators have utilized steering and transport conventions, for example, Directed Diffusion.

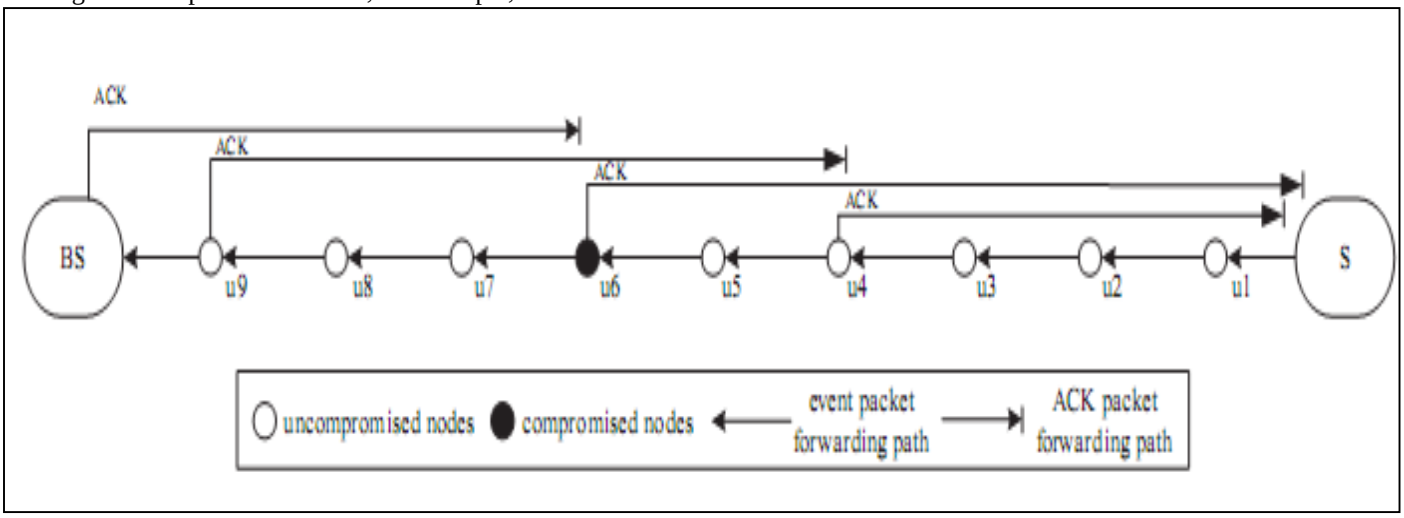

Fig. 1: An example of multihop acknowledgement. Node u4, u6, u are selected as checkpoint

1) CHEMAS: Identify suspect nodes in selective forwarding attacks

A technique for identifying suspect nodes in selective forwarding attack Procedure for identification of specific sending assault is named as CHEMAS (checkpoint-based multi-jump affirmation conspire). This plan arbitrarily select piece of moderate hubs along a sending way as checkpoint hubs which are in charge of creating affirmations for every bundle got. What's more hub needs a restricted hash key chain for guaranteeing the genuineness of bundles. Defer components are likewise created to send current one-way hash key. Each halfway hub in a sending way can possibly recognize irregular bundle misfortune and distinguish presume hubs on the off chance that it doesn't get enough affirmations from the downstream checkpoint hubs.

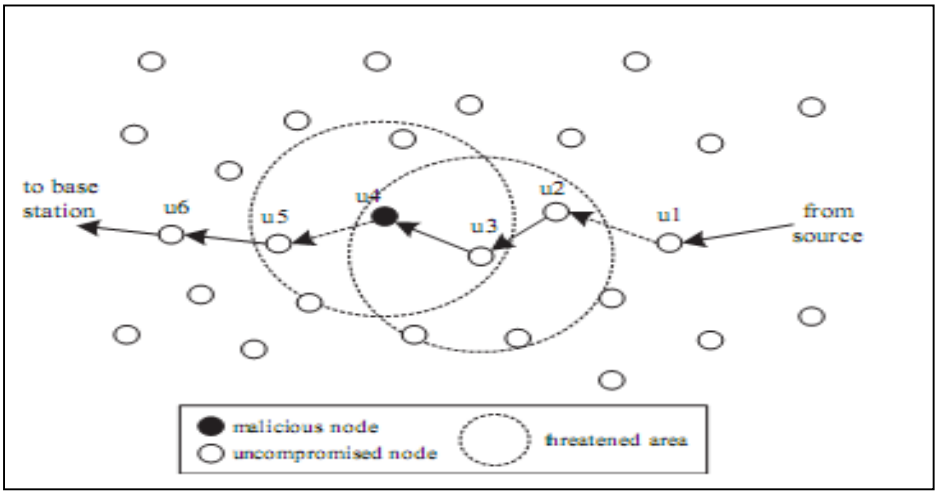

Fig. 2: Identification of suspect node

2) Identifying Selective Forwarding Attacks in Wireless Sensor Networks utilizing SVMs

An incorporated interruption discovery conspire in light of Support Vector Machines (SVMs) and have utilized sliding windows for dark opening assaults and particular sending assaults. In this plan they just recognize the assaults. This plan utilizes steering data nearby to the base station of the system and raises cautions in view of the 2Dfeature vector (bandwidth, hop count). Order of the information examples is performed utilizing a one-class SVM classifier. They use anomaly recognition as base for their plan. Peculiarity recognition flags an interruption when the watched exercises contrast fundamentally from those for the most part embraced by the client.

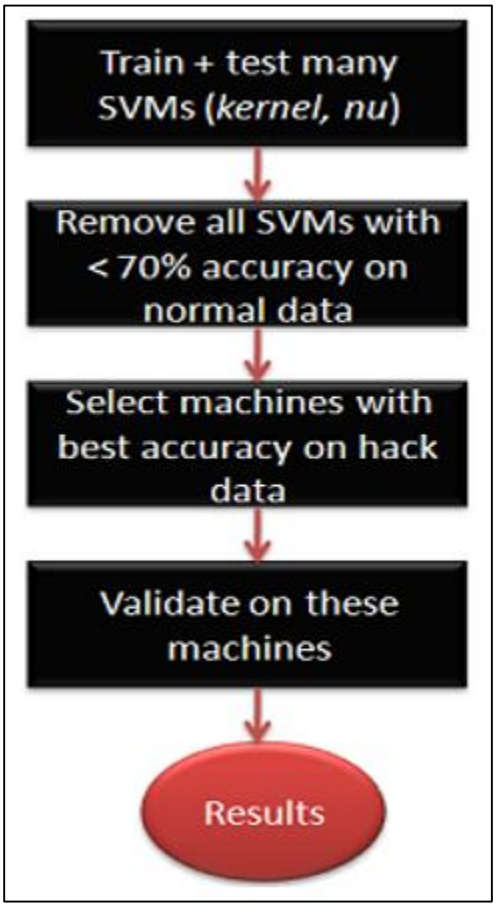

Fig. 3: SVM Selection Process

3) Fuzzy-Based Reliable Data Delivery for Countering selective Forwarding in Sensor Networks

A Fuzzy based dependable information conveyance plot for countering specific sending assault which is an enhanced type of Multi-way steering strategy. The upgrade is that the quantity of transmission way changes with number of aggressor.

4) Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks

A conveyed lightweight barrier plot against particular sending assault, which depends on a hexagonal WSN work topology. This plan uses the neighbor hubs to screen the transmissions of the occasion parcel and recognize specific sending assault by observing bundles' sending of two hubs in the transmission way, and resend these bundles dropped by the aggressors to the goal hub.

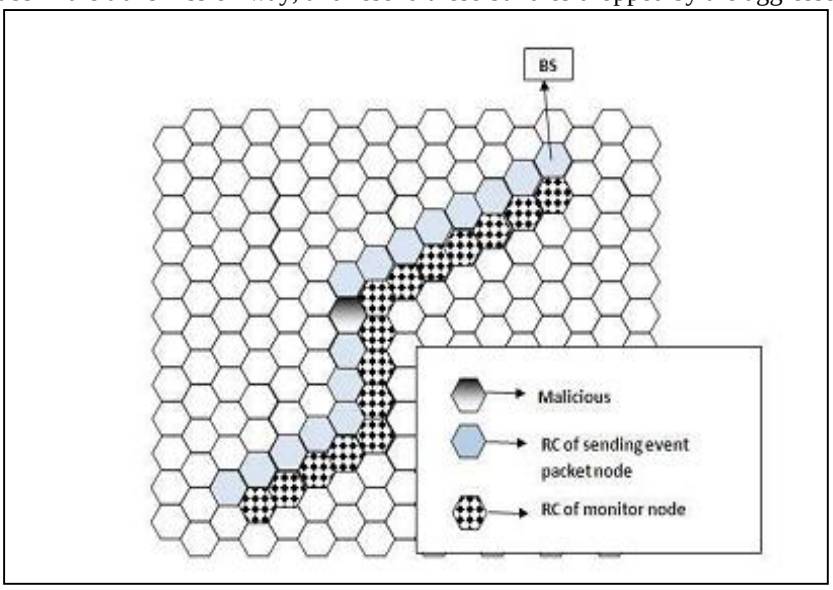

Fig. 4: conveyed lightweight barrier plot

5) Proposed Prevention Technique

I we proposed an efficient defensive scheme against 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 broadcast nature of sensor networks. Instead of discarding the packets, node monitors whether destination is forwarding the packet or not.

IV. RESULTS AND IMPLEMENTATIONS

A. NS2 Network Simulator

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

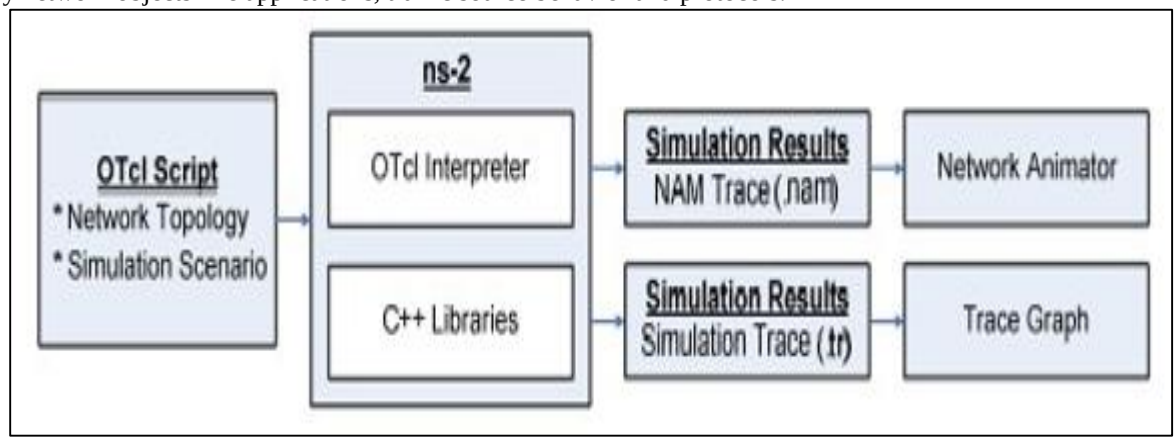

Fig. 5: Working process of ns2 simulator

1) Packet Delivery Ratio

Within the sight of noxious hub is higher on the proposed plot. This is expected to the way that in the proposed conspire a hub chooses a put stock in downstream to convey a parcel to the sink hub. If there should be an occurrence of a bundle misfortune it retransmit to the following most trusted download interface.

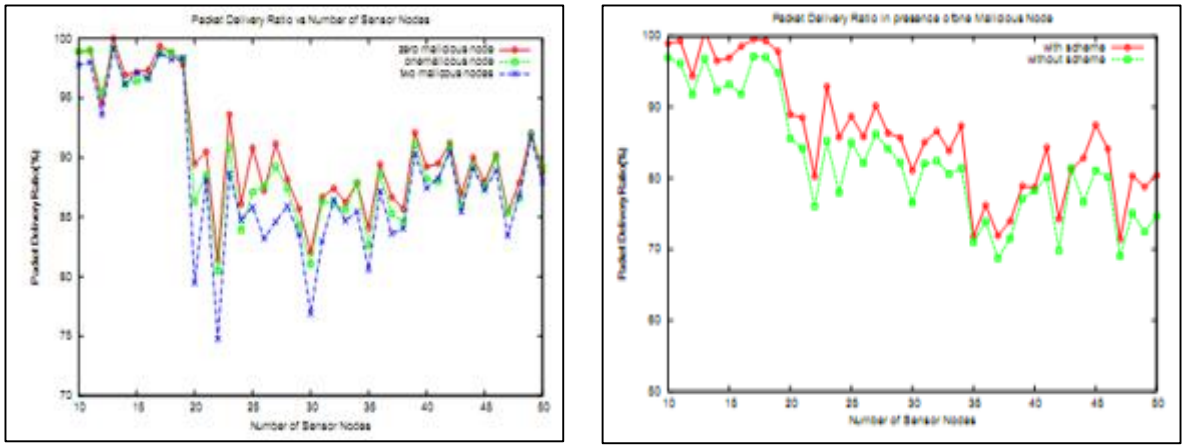

Fig. 6: Packet Delivery Ratio vs Number of Sensor Nodes in presence of one Malicious Node

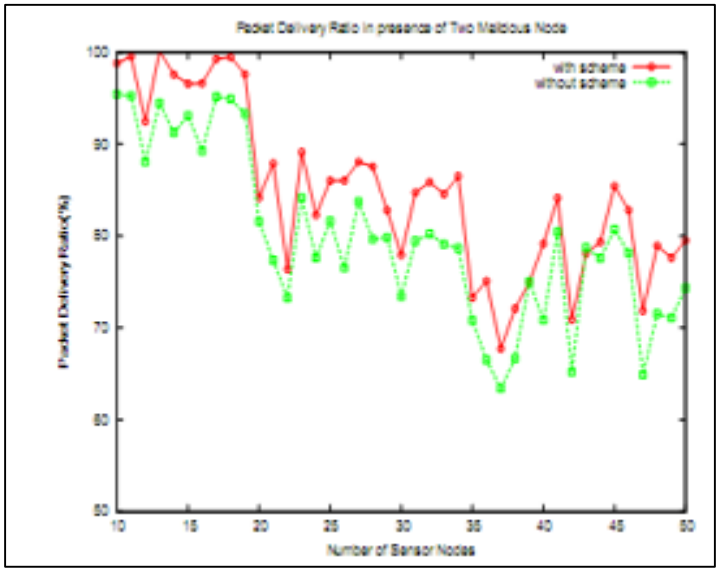

Fig. 7: Packet Delivery Ratio versus Number of Sensor Nodes in nearness of two Pernicious Node

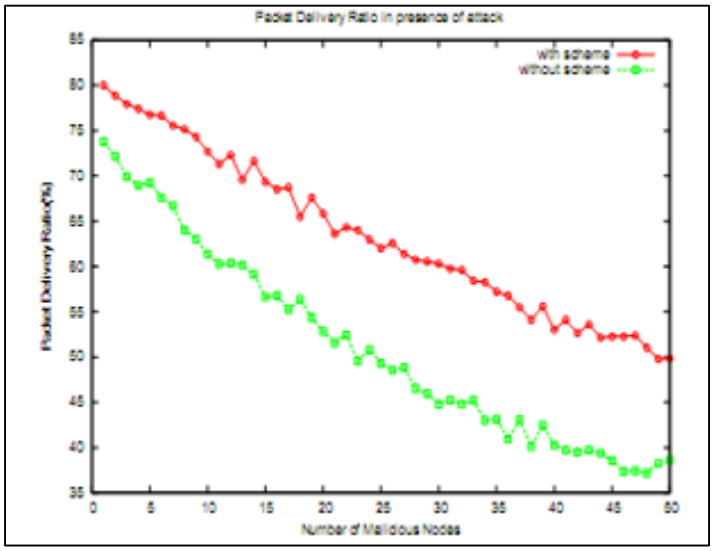

Fig. 8: Parcel Delivery Ratio versus Number of Malicious Node for a system of 100 hubs

V. CONCLUSION

For data transmission, we use multi-hop system. In multi-hop system from which route, we transmission our data is an issue. For selecting route among multi-hop and multiple path, known as Routing. Routing security is an important issue in WMN as well as other wireless network. We needs to consider a better tradeoff between higher security and network performance while designing of 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. In terms of communication overhead, our scheme is more efficient than typical multipath schemes. In addition, by utilizing an existing routing protocol .which is secure against sinkhole attacks, our scheme also provides security against sinkhole attacks. With a specific end goal to diminish the correspondence overhead and in addition to spare the devouring vitality in every sensor hub, we can convey bundles ordinarily in a recreation day and age, just enacting the location plot in some delicate interims. A few potential methodologies stay to be taken to enhance the resistance abilities of our plan. For example, utilization of downstream identification would help the base station to gather ready data; the fuse of appropriate repetition.

REFERENCES

[1] CIanF. Akyildiz, XudongWang, Weilin Wang, Wireless Mesh Network: a survey, 1-5, 28-29 Dec. 2010
[2] A.Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, M. Turon,"Routing protocol in Wireless mesh network: challenges and design considerations" , In Proc. Springer Science LLC 2006.pp. 285-303.
[3] Specially appointed On-Demand Distance Vector (AODV) Routing (2003, Febru-ary) http://www.ietf.org/web drafts/draft-ietf-manet-aodv-13.txt 4 A. Iwata, C.- C. Chiang, G. Pei, M. Gerla, and T.- W.Chen, "Versatile Routing Strategies for Ad Hoc Wireless Networks, IEEE Journal on Selected Areas in correspondences, Special Issue on Ad-Hoc Networks, pp.1369-79, Aug2011 [4] YS.R. Das, C. E. Perkins and E. M. Royer, "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, March 2011.
[4] A. Boukerche, "Performance evaluation of routing protocols for ad hoc wireless networks, Mobile Networks and Applications" ,Vol.9, No.4, pp.333342,2013
[5] Wu]V. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proc. IEEE INFOCOM 11, Kobe,Japan (2011)
[6] H.M. Nyo and P. Viriyaphol, "Detecting and Eliminating Black Hole in AODV Routing", IEEE, Jan 2011, pp.1-4.