ijecs
open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 20033-20036
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.35

Behaviour analysis of STREE, SABR and SARDS under different simulation enviornements:A Case Study.

Roopashree H.R., Dr. Anita Kanavalli
Research Scholar Christ University
Bangalore, India
roopashree.r@res.christuniversity.in
*Prof*essor & Head
Department of Computer Science and Engineering
MS Ramaiah Institute of Technology
Bangalore, India
anithak@msrit.edu

***Abstract*—The Wireless Sensor Network (WSN) has been continuous target for research because of Its potential use in data collection Techniques in different hostile and un secured environments. Various techniques and Methods has been explored by different researchers in the area of minimizing energy efficiency and maximizing security concerns in WSN, But still It is one of the key area to look further. In future WSN will be connected to Internet of Things (IoT) so researches need to study the behavior of proposed techniques in different simulation environments. In this paper we have case studied and shown the our earlier proposed Techniques i.e. STREE,SABR and behave in different simulation environments.**

Keywords-component; Wireless Sensor Network, STREE, SABR, SARDS, Mobile Node

I. INTRODUCTION

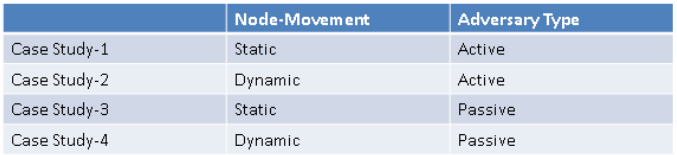
A wireless network is type of network that connects various computing devices (server machines, client machines) along with other hardware (printers). This is the best cost-effective alternative for wired network that ensure better reachability and extremely less maintenance issues.. The present paper basically emphasize behavior of different protocols i.e,STREE,SABR and SARDS under different simulation enviornemts. Section II discusses about some of the recent techniques for energy efficiency as well as security incorporations on different techniques. Section III briefly discusses the result obtained during simulation study. And last section discuss the conclusion.

II. RELATED WORK

There are various research work that have been performed towards increasing energy efficiency as well as increasing security in wireless sensor network. Roopashee et al.[1] done extensive literature survey on existing security and energy efficient on different existing hierarchical protocol and Identified research gap, from the research gap author published a research paper [2] in this author introduced a novel hierarchical technique “STREE: A Secured Tree based Routing with Energy Efficiency in Wireless Sensor Network” using clustering approximation along with lightweight key broadcasting mechanism in hierarchical routing protocol. The outcome of the study was compared with standard SecLEACH to find that proposed system ensure better energy efficiency and security also author presented a paper [3] novel routing protocol called as SABR (Secured Authentication based Routing) algorithm paper performs an effective authentication process for all the sensor nodes involved in communication process in WSN. The data packet is digitally signed and uniquely encrypted, which upon performing a secure handshaking mechanism authenticates both the node involved in routing process. The design principle of the proposed system is totally applicable on large scale WSN, where the outcome is found with fail-proof authentication system with efficient compliance of computational complexity. Further author paper presents a technique [4] called as SARDS (Secured Anonymous Routing with Digital Signature) that performs verification of the routing information exchanged among the sensors in Wireless Sensor Network. SARDS uses elliptical curve cryptography as the backbone of security formulations and performs authentication of all the communicating nodes present in the network. Finally author [5] proposed a schema that jointly mitigates all techniques.

III. RESULT DISCUSSION

For the purpose of performing comparative analysis, Four different case studies have been conducted to study the behavior of the protocols STREE, SABR and SARDS. Below are the four different case studies done.



	Node-Movement	Adversary Type
Case Study-1	Static	Active
Case Study-2	Dynamic	Active
Case Study-3	Static	Passive
Case Study-4	Dynamic	Passive

1. Node-Movement: This is the first variable used in the case study where the Node moment can be static or Dynamic.

DOI: 10.18535/ijecs/v6i1.35

a. Static nodes are to simulate the applications where WSN nodes are not mobile ex: Area monitoring, Forest fire detection, Structural health monitoring, Machine health monitoring

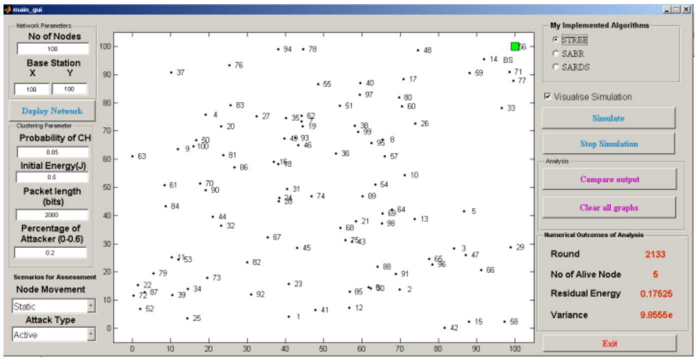
b. Dynamic nodes are to simulate the application where WSN nodes are mobile example: Habitat monitoring, Autonomous Vehicles monitoring, Unmanned Vehicles monitoring.

2. Attack Type: Two types of attacks are targeted here, one is Active attack and another is Passive attack

a. Active: An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

b. Passive: A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target

All four case studies are applied to STREE, SABR and SARDS where the performance of each are measured with respect to the Number of alive nodes, Residual energy, Throughput and Variance of Energy


main_gui

Network Parameters
No of Nodes: 100
Base Station X: 100 Y: 100
Deploy Network

Clustering Parameter
Probability of CH: 0.05
Initial Energy(J): 0.5
Packet length (bits): 2000
Percentage of Attacker (0-0.6): 0.2

Scenarios for Assessment
Node Movement: Static
Attack Type: Active

My Implemented Algorithms
● STREE
○ SABR
○ SARDS

☑ Visualise Simulation

Simulate
Stop Simulation

Analysis
Compare output
Clear all graphs

Numerical Outcomes of Analysis
Round 2133
No of Alive Node 5
Residual Energy 0.17525
Variance 9.8555e

Exit

Figure 1: Node deployment GUI indicating different network parameters.

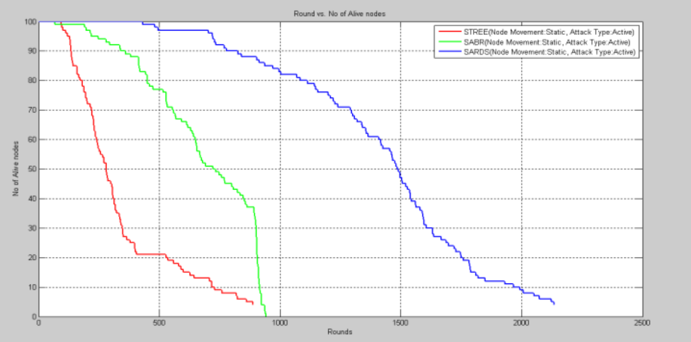


Figure 2: Performance evaluation when node movement Static, Attack Type active vs No.of Alive nodes.

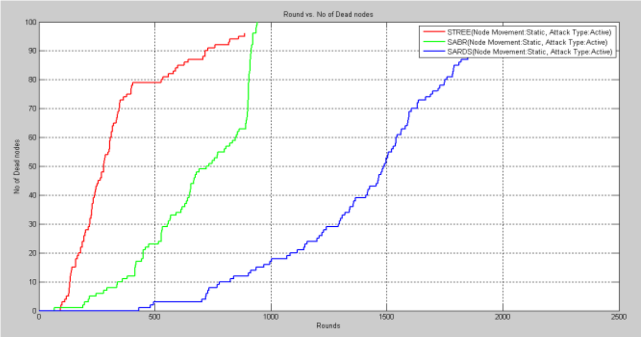


Figure 3: Performance evaluation when node movement Static, Attack Type active vs No. of Dead nodes.

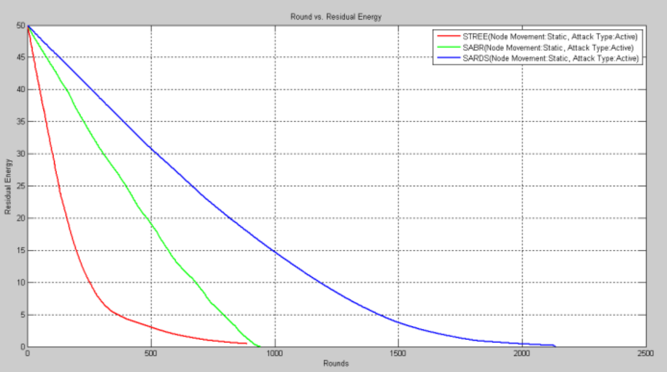


Figure 4: Performance evaluation when node movement Static, Attack Type active vs Residual energy.

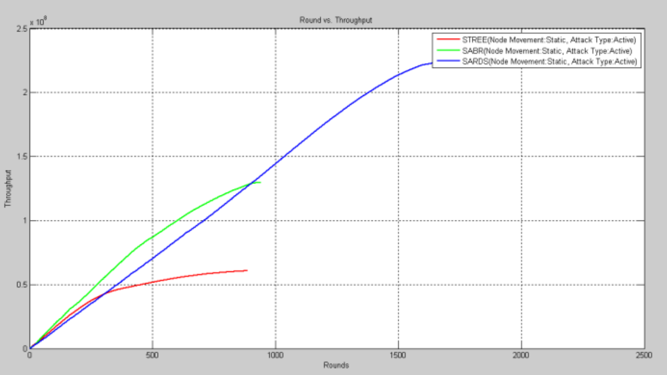


Figure 5: Performance evaluation when node movement Static, Attack Type active vs Throughput

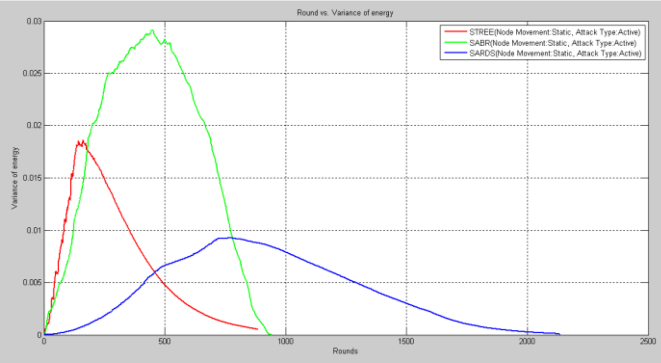
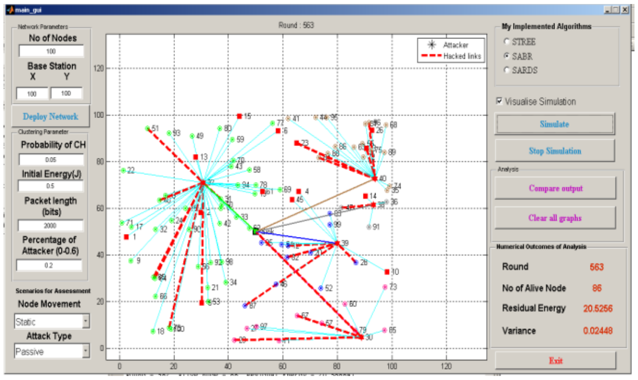


Figure 6: Performance evaluation when node movement Static, Attack Type active vs Variance of energy.



Network Parameters

No of Nodes: 100

Base Station X: 100 Y: 100

Clustering Parameter

Probability of CH: 0.05

Initial Energy(J): 0.5

Packet length (bits): 2000

Percentage of Attacker (0-0.6): 0.2

Scenarios for Assessment

Node Movement: Static

Attack Type: Passive

My Implemented Algorithms: ○ STREE ● SABR ○ SARDS

☑ Visualise Simulation

Numerical Outcomes of Analysis

Round: 563

No of Alive Node: 86

Residual Energy: 20.5256

Variance: 0.02448

Figure 7: Node deployment GUI when Node Movement is static and Attack type is passive.

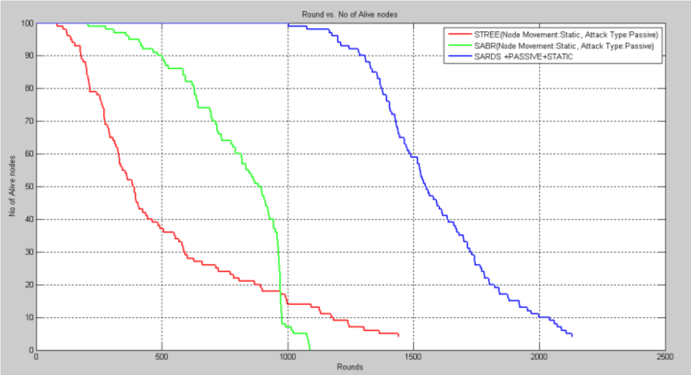


Figure 8: Performance evaluation when node movement Static, Attack Type passive vs No.of Alive nodes.

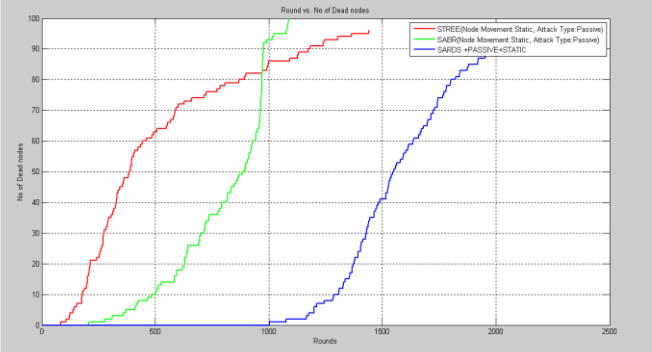


Figure 9: Performance evaluation when node movement Static, Attack Type passive vs No.of Dead nodes.

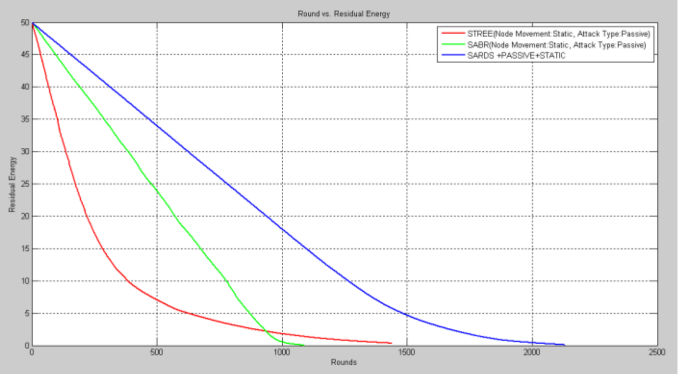


Figure 10: Performance evaluation when node movement Static, Attack Type passive vs Residual energy.

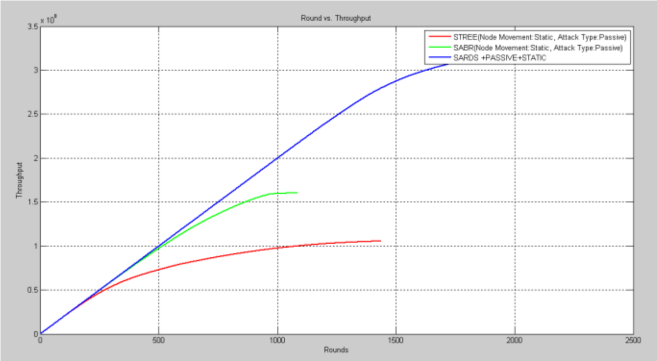


Figure 11: Performance evaluation when node movement Static, Attack Type passive vs Throughput.

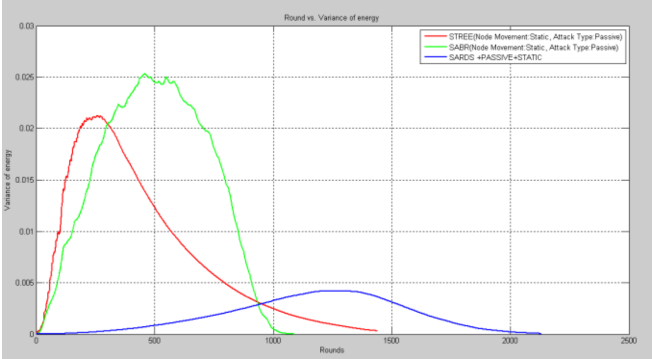
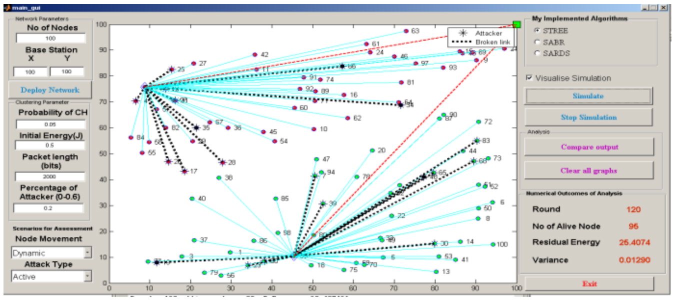


Figure 12: Performance evaluation when node movement Static, Attack Type passive vs variance of energy.



Network Parameters

No of Nodes: 100

Base Station X: 100 Y: 100

Clustering Parameter

Probability of CH: 0.05

Initial Energy(J): 0.5

Packet length (bits): 2000

Percentage of Attacker (0-0.6): 0.2

Scenarios for Assessment

Node Movement: Dynamic

Attack Type: Active

My Implemented Algorithms: ● STREE ○ SABR ○ SARDS

☑ Visualise Simulation

Numerical Outcomes of Analysis

Round: 120

No of Alive Node: 95

Residual Energy: 26.4074

Variance: 0.01290

Figure 13: Node deployment GUI when Node Movement is Dynamic and Attack type is Active.

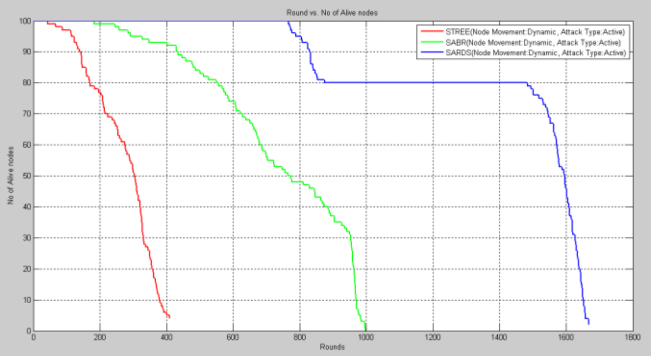


Figure 14: Node deployment GUI when Node Movement is Dynamic and Attack type is Active vs No. of. Alive nodes

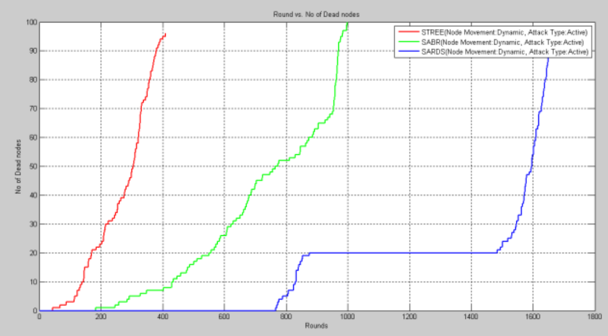


Figure 15: Node deployment GUI when Node Movement is Dynamic and Attack type is Active vs No .of. Dead nodes

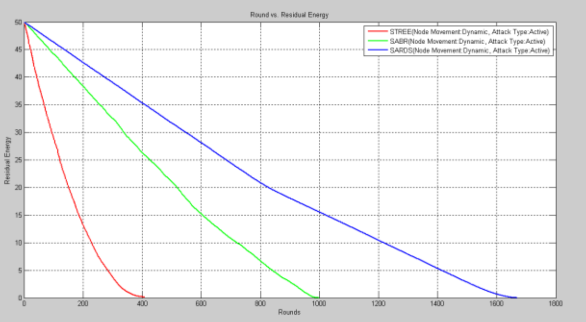


Figure 16: Node deployment GUI when Node Movement is Dynamic and Attack type is Active vs Residual energy.

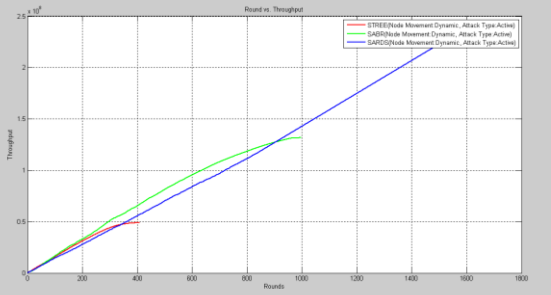


Figure 17: Node deployment GUI when Node Movement is Dynamic and Attack type is Active vs Throughput

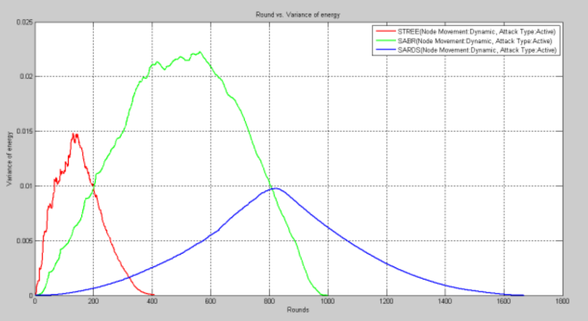


Figure 18: Node deployment GUI when Node Movement is Dynamic and Attack type is Active vs variance of energy.

CONCULSION

The above result shows different case studies under different simulation environments. Various performance evaluations is done and result is compare with different techniques.

REFERENCES

[1] H.R. Roopashree, A. Kanavalli, "Study of Secure and Energy Efficient Hierarchical Routing Protocols in WSN", International Journal of Engineering Research & Technology, Vol. 3 Issue 6, June – 2014.

[2] H.R. Roopashree, A. Kanavalli, "STREE: A Secured Tree based Routing with Energy Efficiency in Wireless Sensor Network," IEEE International Conference on Computing and Communications Technologies, pp.25-30, 26-27 Feb. 2015.

[3] H.R.Roopashree, A.Kanavalli, "SABR: Secure Authentication-Based Routing in Large Scale Wireless Sensor Network", Springer- Emerging Research in Computing, Information, Communication and Applications, pp.223-229, 2015

[4] H.R. Roopashree, A. Kanavalli, "SARDS: Secured Anonymous Routing with Digital Signature in Wireless Sensor Network", Indian Journal of Science and Technology, Vol 9(7), DOI: 10.17485/ijst/2016/v9i7/85760, February 2016

[5] H.R. Roopashree, A. Kanavalli, "Joint Algorithm for Energy-Conservation and Secure Key Generation in Wireless Sensor Network", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 11, Number 4 (2016) pp 2250-2257.