VOL. 12, NO. 1, JANUARY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ANONYMOUS SECURE RELAY BASED ROUTING PROTOCOL IN WIRELESS SENSOR NETWORK

Srinivasan R. and E. Kannan
Department of Computer Science and Engineering, Vel Tech University, Chennai, Tamil Nadu, India
E-Mail: Srinivasanrajkumar28@gmail.com

ABSTRACT

Present network communication protocol in wireless sensor network posses wide range of security vulnerabilities in routing data packets between the hops or base station (Server). It is impossible to detect such vulnerabilities and attackers exploit these vulnerabilities in order to penetrate into the network. Many researchers and security forum focus to overcome such vulnerabilities in routing mechanisms and existing security mechanism fails to handle this flaw in terms of secured routing. In this paper, a novel anonymous secure relay based routing (ASRR) approach is proposed in order to overcome some limited data theft. The key idea is to establish the communication channel between the hops using secure relay. Then to anonymize the entire network relays using circuited multi route protocol. The proposed protocol is experimentally tested and validated using python in a sandboxing environment.

Keywords: anonymous, routing, WSN, data theft, secure relay.

INTRODUCTION

The unique characteristics in Wireless Sensor Network are its standalone and clustered behavior. Hence existing security mechanism available for general network cannot be applied for WSN. Present day attacks were also in more feasible form and outreach of the node information, node identity and network identity is very large when compared to previous decades [5]. Hence in the research area of sensor network routing, performance, integrity, confidentiality is vital other than it anonymity were also into consideration [7]. All the attack vectors and strategies were followed and being practiced in the area of sensor network. These attacks can be prevented using some detection and prevention security mechanism; in complement to it a novel approach of Anonymisation is proposed [1].

The paper is structured as follows; section 1 gives an overview about sensor network, section II dealt with related works about the existing literature. Section III introduces the novel idea and section IV elaborates the experimental setup and experimentation. Section V states the performance analysis carried out by the proposed protocol with other existing protocols. Finally paper concludes with the achieved results and general discussion towards future.

RELATED WORKS

Traditional protocol modification in order to achieve security may help to an extend but full security achievement is impossible [2]. Ganesh *et al* proposed a routing scheme by modifying the AODV protocol using Signal to Noise ratio. Here the author contributes better in terms of dynamic clustering approach however the existing protocol modification can help the security issues which were available and well known [3-6]. Attack vectors in new form can easily penetrate into the network. Roy et al proposed another scheme using secure data aggregation, here the scheme uses secure multipath in order to achieve multipath routing. However the data aggregation leads to lead fusion and fusing multiple data from multiple nodes can cause the system to failure and leads to disaggregation of compromised nodes.

Liu [8] proposed an approach on Secure and Energy efficient multipath routing scheme. The scheme comprises with secure secret sharing among the sensor nodes. The proposed scheme by Liu increases the multipath network lifetime and security features. However the method lacks in terms of presharing the secret among the nodes or clusters. The attacker may compromise the legitimate node and can impersonate as legitimate using shared secret.

Yang et al proposed a anonymous routing protocol named NUCPP. The key idea of this protocol is to use Uncorrelated Pseudonym pairwise mechanism instead of using Pseudonym node correlation properties. Author adopts the intra circular routing scheme properties to achieve full Anonymisation [1].

Proposed - anonymous secure relay based routing

In order to overcome the above stated issues in routing protocols and in order to increase the security mechanism in wsn routing, a novel ASRR protocol is proposed. The protocol consists of two main phased namely i) Secure relay phase, where the secure relay is established between the hops for secure data transmission ii) Anonymisation, where these secure relay gets anonymised.

Secure relay

In general secure relay is an agent based port forwarding services carried out to achieve security in data exchange. Here the approach of the same is used with individual standalone agents deployed along with sensor nodes in the whole network. These agents take care of performing the secure relay connections between the nodes. Whereas this agent maps the MAC addresses of each node in order to perform secure connection and route establishment. The routing performed by the proposed protocol is not as same as existing routing schemes available in sensor network but it differs where the node

identity is fully anonymised and randomness is created using node heads or cluster heads.

Anonymity

Anonymisation is achieved for both the node and network level. The node Anonymisation is where the entire node identity is hidden and network Anonymisation stands for network path or link level Anonymisation. The Anonymisation of network level plays a major role. Here the entire path is circuited by means of circuit level route switching is achieved. The key idea behind the process stands, initially the node information is taken and randomness is created for node anonymity using Galois Finite field number. Then these random generated values where equally shuffled down. Then the nodes with same enclosed identity which belongs to various networks were taken into consideration. These node with secure relay path were obtained and circuited with multiple paths. These circuits were framed based on multiple network entities where the node information was passed between these circuits.

EXPERIMENTAL SETUP

In order to test and validate the proposed protocol, an experimental setup was created. Experimentation was carried out for 11 hybrid sensor nodes with both homogenous and heterogeneous functionalities. Nodes 1, 2, 5, 7, 8 were homogeneous nodes with basic configuration of motes while nodes 3, 4, 6, 9, 10, 11 were heterogeneous configuration. The protocol test bed is fully developed using python 2.7 with the supported module flask, panda, numpy and scipy. Some of the native dependable modules were also used but they were more specific to native binaries. The link with Pink color shows the active relay connection between multiple hop nodes. Here the entire setup is anonymised and the node which transmitting the data and receiving the data from other hops will be intimated in run time only. The relay established its secure route in terms of forming circuits which is mentioned in the Figure-1. These circuits are randomly scattered and formed according to the randomness possessed by the nodes.

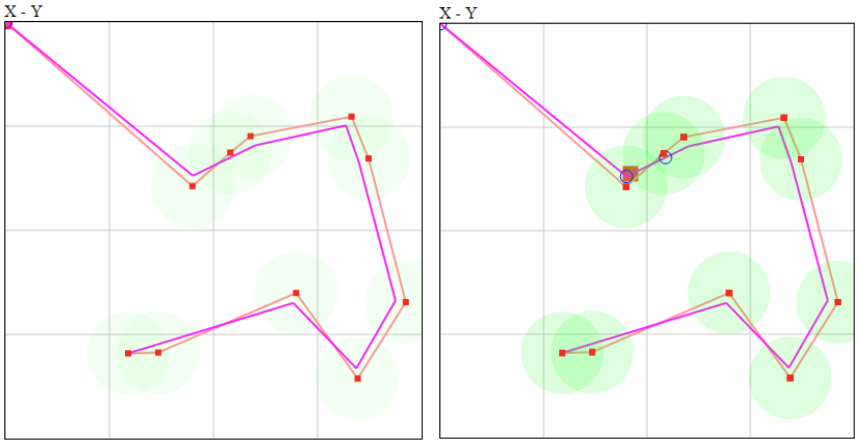
Algorithm

(Assumption: Maximum number of nodes was splitted into multiple networks, where a network can hold only maximum of 50 nodes).

Begin

Initialize the node identity with randomness
Apply GF (prime)
Shuffle the random values
Randomly pick 50 possible nodes from different network
Establish secure relay
Make a circuit
Establish connection
Perform routing (Secure relay, circuit)

End



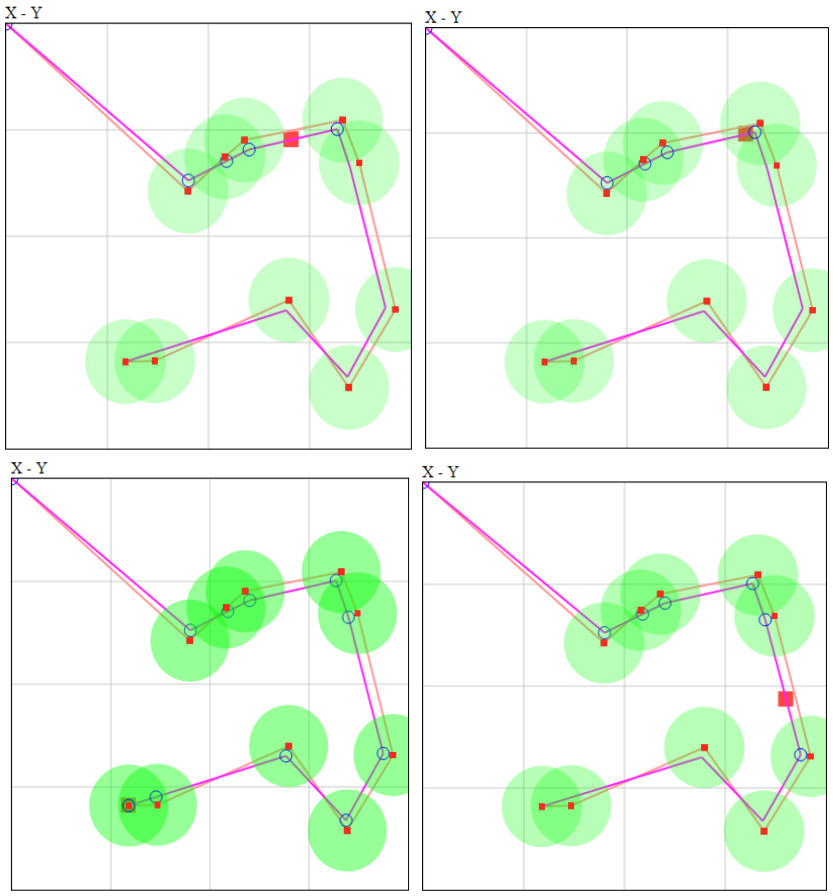


Figure-1. Simulation results with anonymous secure relays.

Performance analysis

In order to validate the performance of the proposed protocol varies features were taken into consideration. Some of the features taken were Throughput, secure path, circuit delay, hop transformation. The two prominent features circuit delay and hop transformation were considered in order to validate the secure relay and anonymity of the node. Table-1 reflects the performance analysis of sensor nodes with increasing number maximum upto 50 nodes. Table-2 and Table-3 shows the results for secure path establishment and circuit delay. Table-4 shows the information about the hop transformation. The information stated in the table 4 will be on hold by the cluster head in order to achieve full anonymity. The cluster head will forward the particular hop transformation information in runtime only. The performance of the proposed protocol is compared with RAEED and STREE where the proposed protocol performs better.

Table-1. Throughput.

S. No.	Number of nodes	Algorithm	Approach	Percentage
1	50	TARF	Trust aware	88
2	50	STREE	DDoS Mitigation	89
3	50	ASRR	Anonymity	93

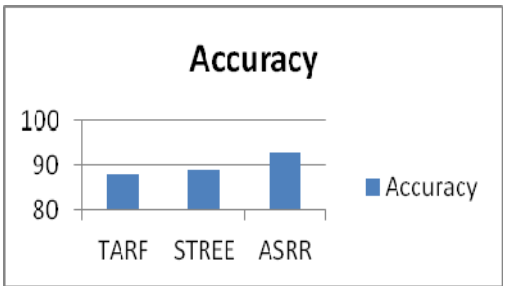


Table-2. Secure path.

S. No.	Number of nodes	Algorithm	Technique	Path
1	50	TARF	Trust aware	60
2	50	STREE	DDoS Mitigation	58
3	50	ASRR	Anonymity	60

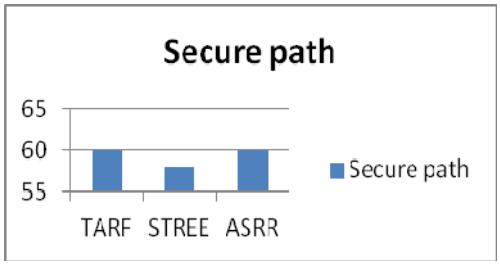


Table-3. Delay.

S. No.	Number of nodes	Algorithm	Technique	Delay in ms
1	50	TARF	Trust aware	0.06
2	50	STREE	DDoS Mitigation	0.2
3	50	ASRR	Anonymity	0.03

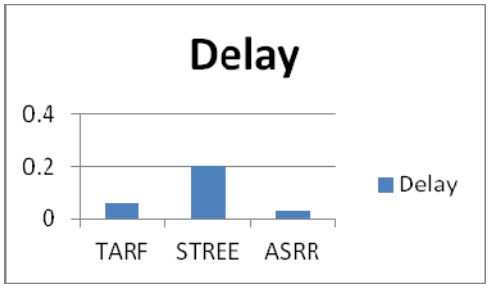


Table-4. Hop transformation.

S. No.	Number of nodes	Algorithm	Technique	Hop transformation (%)
1	50	TARF	Trust aware	-
2	50	STREE	DDoS Mitigation	-
3	50	ASRR	Anonymity	40

CONCLUSIONS

Hence the paper is concluded by proposing the novel secure relay based protocol to perform secure routing. The idea is novel and hence it can be adopted to any sort of wireless networks. The proposed approach is more inevitable to support both heterogeneous and homogenous network. From the experimentation, the conclusion can be derived as the protocol is more stable in any network and the route establishment is fully anonymised. The only drawback of the proposed protocol is, when a node failure happens it takes time to reform the circuit and network identity. Hence it is not easy sniff the path by any attacker. In future, some cryptographical algorithms and existing authentication protocol can be used to validate the security in routing. Cryptographical techniques can be incorporated to encrypt the traffic moving in and around the sensor network.

REFERENCES

[1] G. Yang, G. Geng, J. Song, Z. Liu, H. Han and X. Gao. 2013. A secure anonymous routing protocol in WSN. Information and Automation (ICIA), 2013 IEEE International Conference on, Yinchuan. pp. 415-418.

[2] Roopashree H. R. and A. Kanavalli. 2015 STREE: A Secured Tree based Routing with Energy Efficiency in Wireless Sensor Network. Computing and Communications Technologies (ICCCT), 2015 International Conference on, Chennai. pp. 25-30.

[3] S. Ganesh and R. Amutha. 2013. Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. In Journal of Communications and Networks. 15(4): 422-429.

[4] S. Roy, M. Conti, S. Setia and S. Jajodia. 2014. Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact. In IEEE Transactions on Information Forensics and Security. 9(4): 681-694.

[5] A. Selcuk Uluagac, R. A. Beyah and J. A. Copeland. 2013. Secure Source-Based Loose Synchronization (SOBAS) for Wireless Sensor Networks. In *IEEE* Transactions on Parallel and Distributed Systems. 24(4): 803-813.

[6] G. Zhan, W. Shi and J. Deng. 2012. Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs. in IEEE Transactions on Dependable and Secure Computing. 9(2): 184-197.

[7] W. Gu, N. Dutta, S. Chellappan and X. Bai. 2011. Providing End-to-End Secure Communications in Wireless Sensor Networks. in IEEE Transactions on Network and Service Management. 8(3): 205-218.

[8] A. Liu, Z. Zheng, C. Zhang, Z. Chen and X. Shen. 2012. Secure and Energy-Efficient Disjoint Multipath Routing for WSNs. in IEEE Transactions on Vehicular Technology. 61(7): 3255-3265.