Cluster Computing
https://doi.org/10.1007/s10586-017-1512-1

Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: a trust-aware routing framework for wireless sensor networks

M. Udhayavani[1] · **M. Chandrasekaran**[2]

Received: 23 September 2017 / Revised: 30 November 2017 / Accepted: 12 December 2017
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
A wireless sensor networks encompasses battery powered sensor nodes with extremely limited processing capabilities. One of the major challenges in WSN is to overcome the attacks like Sinkhole, Wormhole and Sybil, Dos attacks, Selective forwarding etc. which reduces the performance of the network, since the Cryptographic techniques are not much effective in solving this problem. So in order to protect wireless sensor networks from attacks and to perform improvement in some of the aspects we have implemented a low overhead trust aware routing with energy efficient network protocol. This protocol is designed by incorporating the trust aware routing frame work with adaptive periodic threshold sensitive energy efficient network protocol. By minimizing the attacks, the network provides a better QOS with trustworthy and energy efficient route which leads to increase the network life time.

Keywords Wireless sensor network (WSN) · Routing protocol · TARF · TAREEN · Security

1 Introduction

Wireless sensor network consists of spatially distributed sovereign sensors to monitor various conditions like physical and environmental factors in the field. WSN is mostly used in military, industrial and consumer applications and in health monitoring machines. Typically in a WSN application there are two types of nodes: source node—the node which actually senses and collect the data and sink node—the node to which the collected data is to be sent and both of these nodes are responsible for self-organization of an appropriate network infrastructure. The sinks can be the part of the network or outside the wireless sensor network. In most of the applications the sink node does not concern itself with the identification of source nodes but only about the collected data except in situations where it is required to authenticate the source. According to [1] this paper focuses on design of TARF, a robust routing framework for WSNs, to secure multihop routing in dynamic WSNs against harmful attackers a busing the replay of routing information. With the knowledge of trust management, TARF empowers a node to keep track of the trust worthiness of its neighbor to select a reliable route. TARF protects the WSNs by rerunning routing information as it does not require synchronization of time or geographic information. The pliability and scalability of TARF are verified through both extensive simulation and empirical estimation with large-scale WSNs, the evaluation involves static and mobile settings, hostile network conditions, and strong attacks like Wormhole, Sink hole and Sybil attacks. WSNs [2] are mainly suited for applications to military surveillance and forest fire monitoring which comprises battery-powered sensor nodes that send messages to a base station via a multihop path whose routing of WSNs regularly becomes the target of malicious attacks and may damage nodes physically, create traffic collision, omit or misdirect messages in routes, or jam the communication channel by creating radio interference [3].

According to [4], ad hoc networks have been emerged in many forms with the rapid development in wireless technol-

✉ M. Udhayavani
udhram@gmail.com

M. Chandrasekaran
drmcs123@yahoo.com

[1] Department of Electronics and Communication Engineering, Vivekanandha College of Engineering for Women, Elayampalayam, Tiruchengode 637205, India

[2] Department of Electronics and Communication Engineering, Government College of Engineering, Bargur, Tamilnadu, India

Published online: 19 February 2018

ogy. These networks are most suited for military and selected commercial applications. However, security of the network is a major concern. Ad hoc networks are susceptible to the infrastructure absence, wireless links between nodes, limited physical Protection, and the Lack of a centralized monitoring or management, and the resource constraints. During the process of *wormhole attack* a malicious node captures packets from one location and channels them to another node at a distant point, which echoes them locally. The tunnels can be a wired link or a packet encapsulation. From an attacker's perspective, this paper analyzes the different attack modes in detail and suggests complex wormhole attacks to improve the regular wormhole attacks. This paper [5] explores in depth of the most severe attacks against the *sinkhole attack*, and accentuate on strategies that an attacker can follow to successfully launch such an attack. Then it proposes explicit detection rules which can make legitimate nodes become aware of the threat, while the attack is still taking place demonstrating the attack and present some executional details that highlight the effort that an attacker would need to put in order to break into a realistic sensor network.

In sinkhole attacks, a malicious node is prerogative itself to be a base station through replaying all the packets from a real base station [5]. Such a fake base station could decoy more than half the traffic which in turn creates a black hole. The same technique is used in another robust form of attack called *Sybil attack* [6] where an attacker present multiple identities to the network done through replaying the routing information of multiple legitimate nodes. An effective node can also be able to launch these attacks. The harmfulness of such malicious attacks is further provoked by introducing mobility into WSNs and the hostile network conditions. Nevertheless mobility is introduced into WSNs for efficient data collection and various other applications [7–10] it greatly increases the chance of interaction between the honest nodes and the attackers. In addition to that, a meager network connection causes much striving in differentiate between an attacker and an honest node with transient failure. Surprisingly, the existing routing protocols for WSNs an emphasis on energy efficiency [11], and attempt to dismiss unauthorized participation by encrypting data and authenticating packets. Such encryption and authentication schemes for wireless sensor networks were included in [12–15]. It is utmost important to contemplate proficient energy use for battery-powered sensor nodes and the heftiness of routing under topological changes as well as common faults in a wild milieu. Yet, it is precarious to incorporate security as an important goal by replaying routing information even with perfect encryption and authentication, a malicious node can be still able to partake in the network using another valid node's identity. The routing protocols gossiping-based bid convinced protection against the attackers by the selection of random neighbors to forward packets [16], but at a price of ample overhead in propagation time and energy use. Along with the cryptographic methods, trust and reputation management has been employed in generic adhoc networks and WSNs to safe and secured routing protocols. Principally, such a system assigns each node a trust value according to its performance in the past routing. At that juncture, such a trust value will help in decide a secure and efficient route. Still, the proposed trust and reputation management systems for generic ad hoc networks target only on hardware platforms like laptops and smart phones [17–20].

In order to protect WSNs from the harmful attacks exploiting the replay of routing information, we have designed and implemented a robust trust-aware routing framework, TARF, to secure routing solutions in wireless sensor networks. The effectiveness of TARF is verified on large-scale WSN through extensive evaluation with simulation and empirical experiments. Finally, we have implemented a ready-to-use TARF module with low.

Overhead, which as demonstrated can be integrated into existing routing protocols with ease; the demonstration of a proof of-concept mobile target detection program indicates the potential of TARF in WSN applications.

2 Routing protocols in WSN

Figure 1 represents the Routing protocols for WSNs include Data-centric Protocols, Hierarchical protocols, and Location Based Protocols.

2.1 Data centric protocol

In this Flooding and Gossiping routings are used. In data-centric protocol both the SPIN and directed diffusion—the congregated data are used to query the data. Sensor Protocols for Information via Negotiation (SPIN) use a naming scheme to define the collected data. Conversely, the mobility of nodes will challenge the speed and adaptability of the SPIN model. In directed diffusion, the sink requests the data from the sensor nodes by communicating the request message. But the problem arises in data-centric approach is that it is best suited for static nodes than with mobile nodes.

2.2 Hierarchical protocol or cluster-based protocol

In wireless sensor network, a collection of sensor nodes into a cluster is well-known as clustering. A cluster head may be selected from the group of the cluster which in turn collects the information from the nodes within the cluster and send this information to the base station (destination). Clustering can be used as energy-efficient communication protocol. The main aim of clustering is to minimize the total transmission power aggregated over the nodes in the selected path and

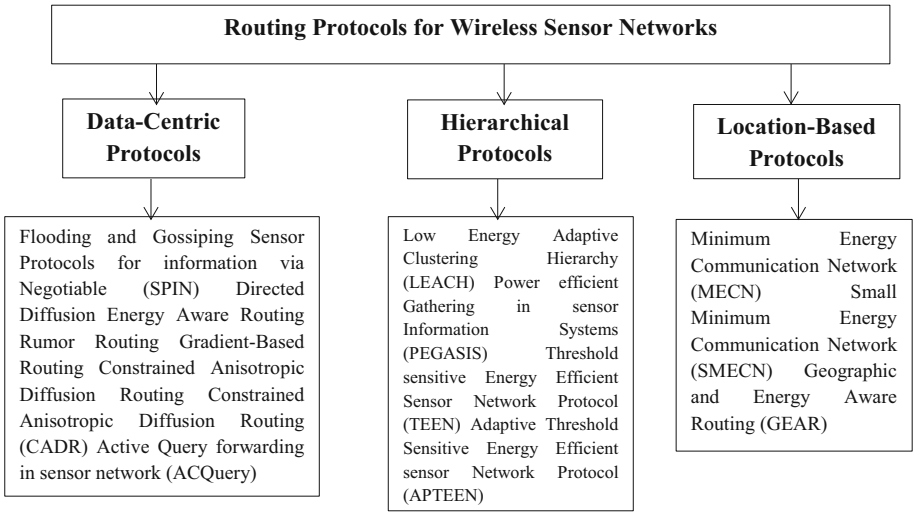


Fig. 1 Routing protocols in WSN

to balance the load between the nodes for extending the network lifetime. LEACH, TEEN, APTEEN, and PEGASIS are few examples of cluster-based protocols where the nodes are grouped and the highly energy consuming node is elected as a cluster head (CH). The cluster head is used to amass the data to the other nodes in its cluster. By using the shortest path algorithm the packets are transmitted from the source node to destination nodes and are easy for managing the routes. These protocols are not suited for time critical applications as it takes more time to compute the cluster heads.

2.3 Location based protocol

Location information is used to perform the energy efficient routing. In order to select the protocol the specific requirements have to be taken into considerations. MECN, SMECN, GEAR are some of the location based protocols. The multi hop routing in WSNs provide little protection against identity deception through replaying routing information because it uses multiple intermediate nodes to reach the destination. The multi hop routing of WSNs often becomes the target of malicious attacks. To protect WSN against harmful attacks efficient routing protocols have been used. The ultimate aim of the proposed work is to minimize the energy consumption and to improve the security. Ad hoc on-demand distance vector (AODV) routing protocol has been designed to provide secure routing information. In the proposed work AODV is used to make sensor nodes and base station communicate with each other. The random number of keys is generated for encrypting and decrypting the routing information. After generating the keys, the pool of keys has to be distributed using different key management schemes.

Reactive protocol is identified as on-demand protocols as it creates routes only whenever these routes are in request. When a source node requires a route to a destination, it inductees a route discovery process within the network and this process will be completed once a route is found or all the possible route permutations have been examined. After that there is a route maintenance procedure to keep track of the valid routes and to eliminate the invalid routes. The most important reactive routing protocol is AODV which is an on-demand and distance vector routing protocol, meaning that a route is established by AODV from a destination only on demand. AODV is capable of both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources capable of both unicast and multi cast routing. The AODV protocol is composed of the two main mechanisms of route discovery and route maintenance which involves the use of route request (RREQ), route reply (RREP) and route error (RERR) messages. A RREQ message is broadcasted when a node needs to discover a route to a destination. Whenever a RREQ reaches the destination node, the destination route is made obtainable by unicasting a RREP back to the source route and the RERR messages is broadcasted for the broken links.

The next step in the proposed work is generation of keys for the sensor nodes and trusted managers. Initially random number of keys are generated and kept in a key pool. The keys generated by using hash function are used for encryption and decryption process involving the use of blowfish algorithm and the keys are distributed to the sensor nodes and trusted manager using different key pre-distribution schemes.

Global mobile information system simulator (GloMoSim) is a scalable simulation library for wireless network systems built using the PARSEC simulation environment (Figs. 2, 3, 4).

Parallel simulation environment for complex systems (PARSEC) is a C-based simulation language used for sequential and parallel execution of discrete-event simulation models.

Operating System : Windows XP
Simulator Tool : GloMoSim
Language : C and JAVA

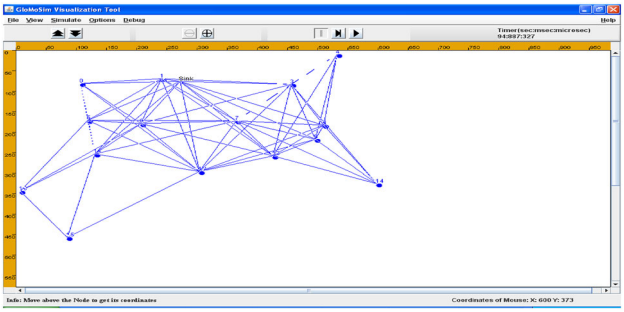


Fig. 2 GloMoSim simulation for routing between nodes

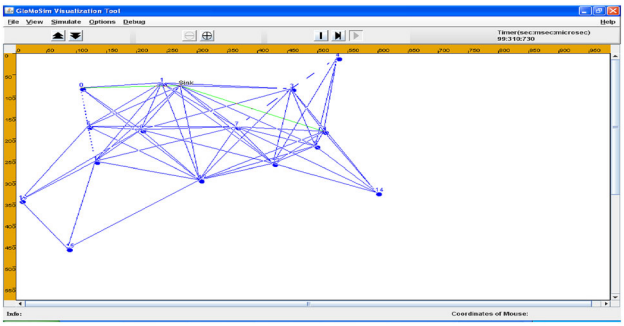


Fig. 3 Simulation showing communication of sink and other nodes

Development Kit : JDK 1.7

Platform : Independent

The wireless sensor networks (WSNs) requires the need of routing protocols and key generation techniques where energy saving and security is a critical issue. To increase the energy efficiency and extend the life time of sensor node, new and efficient energy schemes must be developed. In the proposed scheme, AODV routing protocol is used for communication between the nodes. In this protocol, key generation using hash function is employed. Several trust managers are used to provide security and it also reduces the energy wastage by avoiding multi hop routing where the trust manager acts as the cluster head. The span of wireless sensor networks is prolonged by the use of cluster location and balancing of the network loadings. In this study a cluster-based key management method is proposed that can set a shared key faster and more security using a multiple-key ring assigned to each. This key management method concluded that it can work more energy-efficiently even though the nodes are mobile or new nodes have been inserted. Security analyses indicate that the proposed schemes establish a secure communication with the mobile sink.

3 TARF and TAREEN

In the existing network system, when a file is being sent from base station in such a situation hackers provoked network conditions. The traditional cryptographic techniques effort

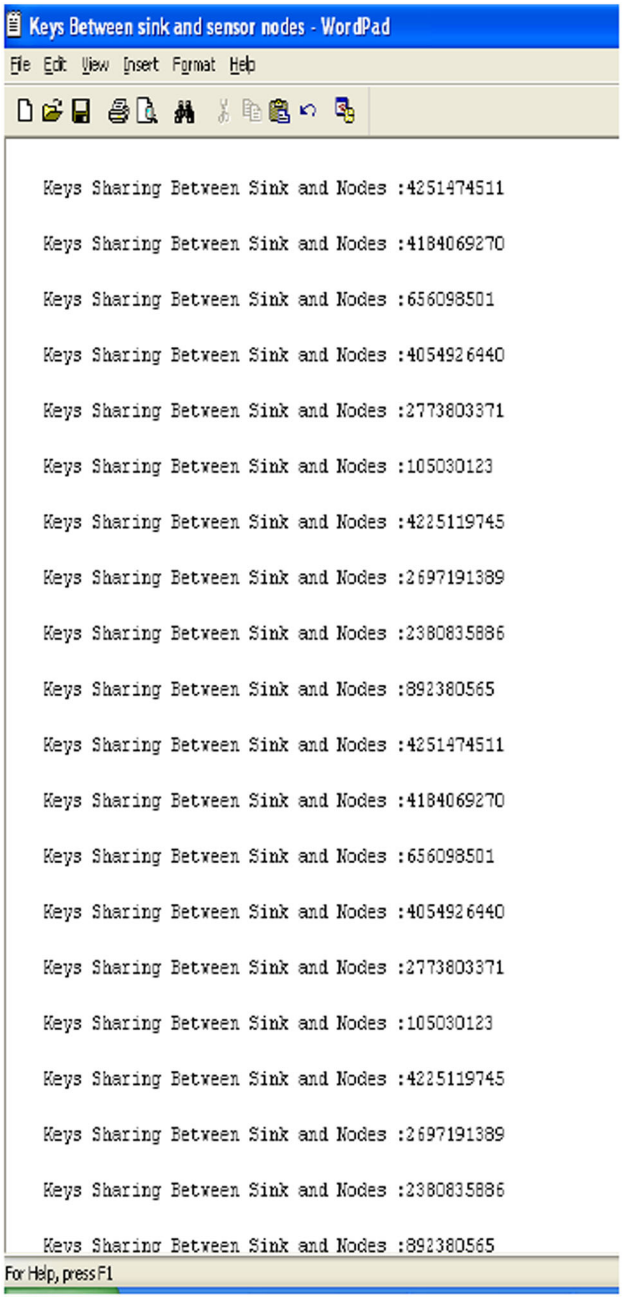


Fig. 4 Simulation showing generated random number of keys

does not discourse the severity of the problems. At that time the file could be exaggerated by the hackers leading to the damage of the network. An attacker may fiddle nodes physically, create traffic collisions, drop out or misdirecting the messages in the routes, or jam the communication channel by creating radio interference.

4 Design consideration of TARF

Trust and reputation management has been employed in Wireless Sensor Network along with cryptographic meth-

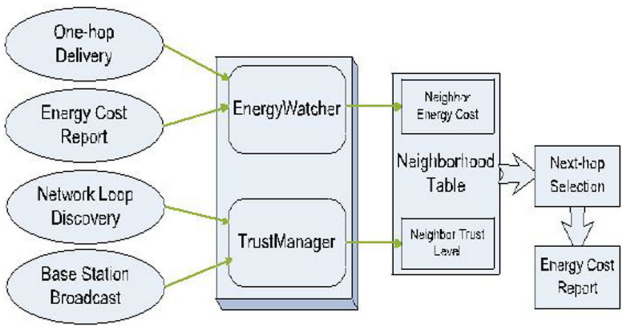


Fig. 5 Each node selects a next-hop node based on its neighborhood table, and broadcast its energy cost within its neighborhood. To maintain this neighborhood table, Energy Watcher and Trust Manager on the node keep track of related events (on the left) to record the energy cost and the trust level values of its neighbors

ods for the security of routing protocols. After analyzing the past performance of each node the system of trust and reputation management assigns a trust value according to it. TARF run on cluster headers only which in turn communicates with other nodes.

In case of TARF Energy watcher and Trust manager are the two important aspects (Fig. 5). Energy watcher is responsible for recording energy cost value of one-hop transmission to reach its neighbors whereas Trust manager is responsible for tracking the trust values of neighbors and the broadcasted messages from the base station.

4.1 TARF with CTP

Although TARF a complete independent routing protocol, it consents the existing protocol to incorporate TARF with least effort and thus makes the protocol to work efficiently. To demonstrate this we incorporated TARF into a collection tree protocol (CTP) which is based on link quality estimation to choose the next node whose main goal is to provide any cast communication.

4.2 TARF with APTEEN (TAREEN)

In the proposed system, trust aware routing with energy efficient networks (TAREEN) focuses on the kind of attacks in which antagonists lead astray network traffic by identity deception with the help of replaying routing information. Based on identity deception the adversary (antagonist) is capable of launching harmful and hard to detect attacks against selective forwarding, wormhole, sinkhole and sybil attacks.

4.3 Routing the network

In this module, the networks embedded on the physical fiber topology. However, assessing the performance reliability achieved independent logical links can share the same physical link, which can lead to correlated failures.

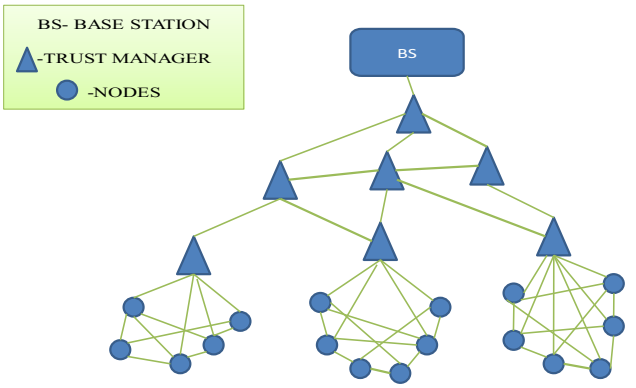


Fig. 6 Hierarchical tree structure-based on the broadcasting range

Mainly, we focus on assessing the reliability of energy level and trusted network. Figure 6 represents the hierarchical tree structure based on the broadcasting range.

4.4 Transfer file

In this module, the shortest path algorithm independently routes each logical link on a physical path with the least number of hops in trusted network basis. The probability of failure of path is minimized when it is routed over the shortest path since we assume that every physical link fails with the same probability. Hence, under the shortest path algorithm, each light- path ravenously takes the most reliable route and transfers the file in secured manner.

4.5 Attacks

Attacks are nothing but the prevention of the base station from obtaining complete and correct sensing data, particularly severe for wireless sensor networks. Most secure or topographical based routing protocols resist to the sinkhole attacks up to a certain level. The Set of sensor nodes unremittingly monitor their surroundings forward the sensing data to a sink node, or base station. An intruder attracts surrounding nodes with unfaithful routing information alters the data passing through it or performs selective forwarding. Many-to-one communications are vulnerable to the sinkhole attack, selective forwarding, wormhole attacks, and sybil attacks.

4.6 Detecting attacks

In most cases it is difficult to identify an attacker who is participating in the network using an id "stolen" from another legal node. For example, it is extremely tough to detect a few attackers colluding to launch a combined wormhole and sinkhole attack. In addition the Trust Manager encourages a node

to choose another route when its current route continuously fails to deliver data to the base station. Our evaluation results indicate that the strategy of switching to a new route without identifying the attacker actually significantly improves the network performance, even with the existence of wormhole and sinkhole attacks.

4.7 Encryption

A different enhanced scheme has to be introduced to improve the lifetime of the wireless sensor network by reducing the energy consumption and also to improve the security. These factors can be fulfilled by developing an energy efficient and trust aware routing protocol. This approach involves the use of level-by-level trust manager.

Here the nodes are grouped based on the energy level. By monitoring the nodes in particular area, the node with highest energy level is assigned as the cluster head and that node acts as the trust manager. The energy level of each node is computed based on its transmission range. For introducing level-by-level trust manager more trust managers are needed. The trust manager count depends and differs by the number of nodes involved, group size and node placement. After establishing level-by-level trust manager, security is enforced by using two different key management schemes. (i) Polynomial pool based key pre-distribution scheme and (ii) Q-composite scheme. There are two types of keys used in this paper: common keys and pair-wise keys.

The common keys are shared by the trust managers to communicate with the other trust manager and the pair-wise keys are used for communication between the nodes and the trust manager. In polynomial pool-based key pre-distribution scheme, each sensor node randomly selects $v$polynomials from a global pool of w polynomials. Any pair of neighboring nodes can calculate a direct pair-wise key if they share the same polynomial. The Q-composite scheme is used to avoid node compromise. The keys are generated using hash function which provides hexadecimal values and they are stored in a key pool. The keys are then distributed to the nodes and the trust manager.

In this paper, we propose an efficient and secured key generation technique for homogeneous WSNs. One way hash function to generate different keys for different sessions and multi path key reinforcement to update the initial generation key and the number of times the hash function will iterate. Although this scheme adds some more communication and computational overhead, the WSN is more secure and resilient to several attacks.

We introduced new protocol developed for hybrid networks, called adaptive periodic threshold sensitive energy efficient network (APTEEN) protocol which is incorporated into TARF (Fig. 7).

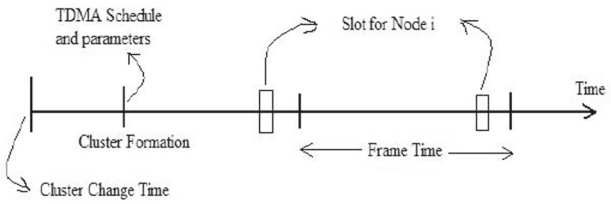


Fig. 7 Timeline for APTEEN

Table 1 Simulation parameters

Simulation time	39.6 μs
Topology size	700 m × 700 m
Number of nodes	03
MAC type	MAC 802.11
Radio propagation model	Free space model
Radio propagation range	250 m
Pause time	0 s
Max speed	4–24 m/s
Initial energy	100 J
Transmit power	0.4 W
Receive power	0.3 W
Traffic type	CBR
CBR rate	512 bytes × 6 per second
Number of connections	01

In APTEEN once the CH is decided it first broadcasts the following parameters: attributes. In these parameters the data are transmitted based on the threshold values. This parameter consists of a hard threshold (HT), soft threshold values (ST) and count time (CT) (Table 1).

HT is a particular value of an attribute where a node can trigger to transmit data. ST is a small change in the value of an attribute which can trigger a node to transmit data again. These parameters are sent to the other sensor nodes in the cluster by the respective cluster heads (CHs). When the sensed data value is greater than the HT, the data is transmitted only when there is a change in that value. Each sensor node in the cluster is given a time slot using a modified TDMA schedule for transmission as shown in Fig. 4. When a sensor node does not transmit data for a time period equal to the CT, it is forced to sense again and re-transmit the data. The APTEEN with TARF is efficient in periodic data transmission and these protocols are suitable for both static and mobile environment.

5 Simulation and results

Simulation is carried out in NS2 for analyzing the route lifetime algorithm the following table shows that the important parameters chosen for the NS2 simulation.

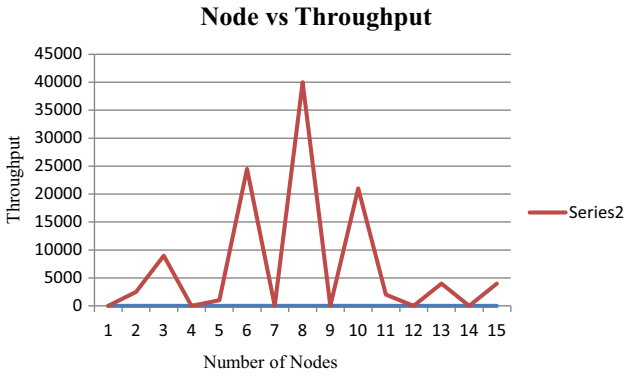


Fig. 8 Throughput (CTP with TARF)

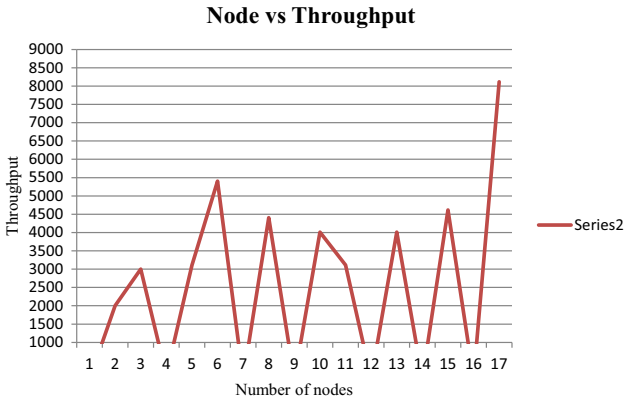


Fig. 9 Throughput (TAREEN)

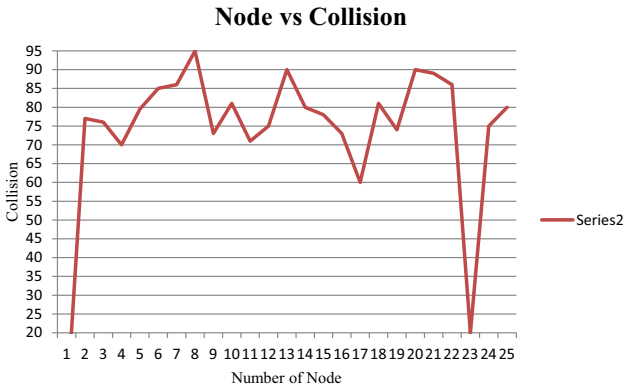


Fig. 10 Collision (CTP with TARF)

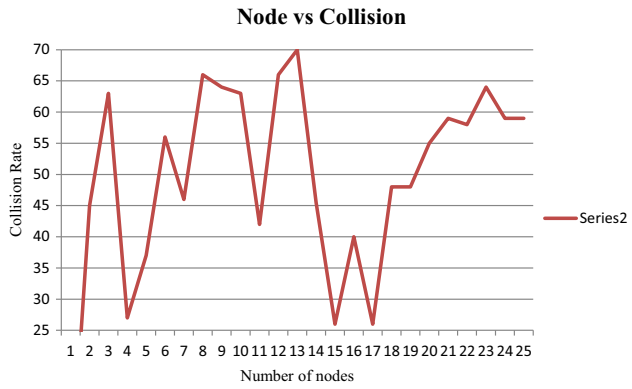


Fig. 11 Collision (TAREEN)

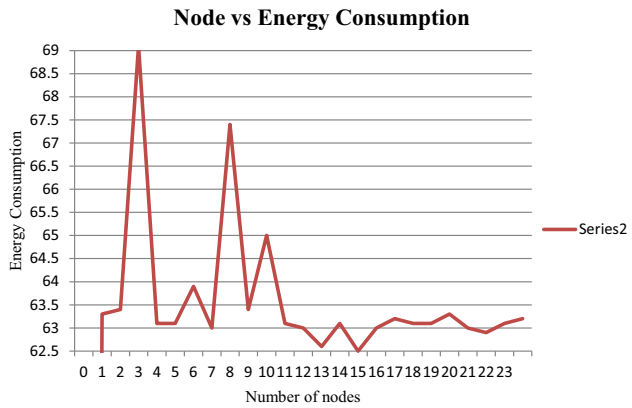


Fig. 12 Energy consumption (CTP with TARF)

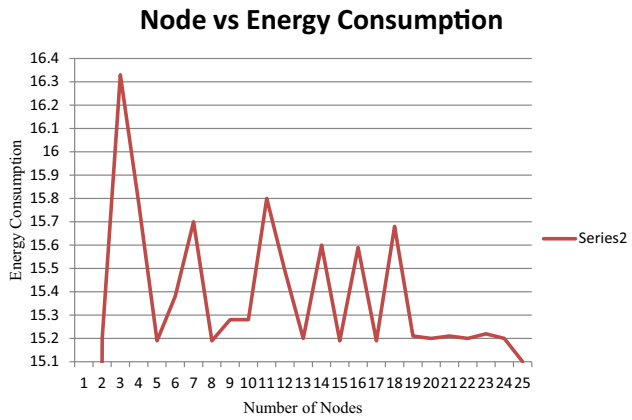


Fig. 13 Energy consumption (TAREEN)

The simulation is performed in NS 2 for various parameters like throughput, collision, energy consumption. From the simulated result it is shown that the performance of TAREEN is high when compared to CTP with TARF. The simulation output is shown by the graph in Figs. 8, 9, 10, 11, 12 and 13. Figures 8 and 9 shows the throughput with TARF and TAREEN, it is evident that even for increased nodes the throughput is maximum and goes on increasing. Figures 10 and 11 shows the collision with TARF and TAREEN similarly Figures 12 and 13 shows the energy consumption.

6 Conclusion

The WSN acquires various security attacks, hence to minimize the attack; TARF is incorporated into collection tree

protocol. But it minimizes only the sinkhole and wormhole attacks and aims only to improve energy efficiency and throughput and it does not include attacks such as selective forwarding and DOS attack and also parameters such as network lifetime and load balance.

But the APTEEN focus on trustworthiness and energy efficiency, this plays vital role in WSN for a hostile environment. It also concentrate in detection of attacks like sinkhole, wormhole attacks, sybil, selective forwarding and DOS attacks and the performance of the network such as latency, load balance are also evaluated. From this evaluation we concluded that the TAREEN produces a better performance in throughput, packet delivery ratio and also it gives a better network lifetime than the CTP incorporated with TARF. It is also efficient in trust aware periodic data transmission and suitable for both static and mobile environment where the CTP incorporated with TARF is suitable only for static environment .

References

1. Zhan, G., Shi, W., Deng, J.: Design and implementation of TARF: a trust-aware routing framework for WSNs. IEEE Trans. Depend. Secure Comput. **9**, 184–197 (2012)
2. Zhao, F., Guibas, L.: Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, Burlington (2004)
3. Wood, A.D., Stankovic, J.: Denial of service in sensor networks. Computer **35**, 54–62 (2002)
4. Jain, M., Kandwal, H.: A survey on complex wormhole attack in wireless ad hoc networks. In: Proceeding of International Conference Advances in Computing, Control, and Telecomm. Technologies (ACT '09), pp. 555–558 (2009)
5. Krontiris, I., Giannetsos, T., Dimitriou, T.: Launching a sinkhole attack in wireless sensor networks; the intruder side. In: Proceedings of IEEE International Conference Wireless and Mobile Computing, Networking and Communication (WIMOB '08), pp. 526–531 (2008)
6. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil attack in sensor networks: analysis and defenses. In: Proceedings Third International Conference Information Processing in Sensor Networks (IPSN '04) (2004)
7. Bai, L., Ferrese, F., Ploskina, K., Biswas, S.: Performance analysis of mobile agent-based wireless sensor network. In: Proceeding Eighth International Conference Reliability, Maintainability and Safety (ICRMS '09), pp. 16–19 (2009)
8. Zhang, L., Wang, Q., Shu, X.: A mobile-agent-based middleware for wireless sensor networks data fusion. In: Proceeding Instrumentation and Measurement Technology Conference (I2MTC '09), pp. 378–383 (2009)
9. Xue, W., Aiguo, J., Sheng, W.: Mobile agent based moving target methods in wireless sensor networks. In: Proceedings IEEE International Symposium Communication and Information Technology (ISCIT '05), vol. 1, pp. 22–26 (2005)
10. Jeong, H.-J., Nam, C.-S., Jeong, Y.-S., Shin, D.-R.: A mobile agent based leach in wireless sensor networks. In: Proceedings 10th International Conference Advanced Communication Technology (ICACT '08), vol. 1, pp. 75–78 (2008)
11. Al-Karaki, J., Kamal, A.: Routing techniques in wireless sensor networks: a survey. Wirel. Commun. **11**(6), 6–28 (2004)
12. Karlof, C., Sastry, N., Wagner, D.: Tinysec: a link layer security architecture for wireless sensor networks. In: Proceeding ACM International Conference Embedded Networked Sensor Systems (SenSys '04) (2004)
13. Perrig, A., Szewczyk, R., Wen, W., Culler, D., Tygar, J.: SPINS: security protocols for sensor networks. Wirel. Netw. J. **8**(5), 521–534 (2002)
14. Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., Kruus, P.: Tinypk: securing sensor networks with public key technology. In: Proceedings Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04), pp. 59–64 (2004)
15. Liu, A., Ning, P.: Tinyecc: a configurable library for elliptic curve cryptography in wireless sensor networks. In: Proceedings Seventh International Conference Information Processing in Sensor Networks (IPSN '08), pp. 245–256 (2008)
16. Safa, H., Artail, H., Tabet, D.: A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wirel. Netw. **16**(4), 969–984 (2010)
17. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)
18. Gong, W., You, Z., Chen, D., Zhao, X., Gu, M., Lam, K.: Trust based routing for misbehavior detection in ad hoc networks. J. Netw. **5**(5), 551–558 (2010)
19. Yan, Z., Zhang, P., Virtanen, T.: Trust evaluation based security solution in ad hoc networks. In: Proceedings Seventh Nordic Workshop Secure IT Systems (2003)
20. Li, J.L.X., Lyu, M.R.: Taodv: A Trusted AODV routing protocol for mobile ad hoc networks. In: Proceedings of Aerospace Conference (2004)
21. Kavita, A.P.: Design and implementation of tarf for WSNs. Int. J. Sci. Res. (IJSR) **3**, 1944–1947 (2012)



M. Udhayavani is working as an Assistant Professor in the Department of Electronics and Communication Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, India. She has completed her Diploma in the field of Electronics and Communication Engineering (DECE) from Valliammai Polytechnic, Chennai. She has completed her Bachelor Degree (B.E.) in the field of Electronics and Communication Engineering from Mahendra Engineering College, Namakkal. She also finished his Post Graduate (M.E.) in the field of Applied Electronics from K.S.R. College of Technology, Tiruchengode. She is the research scholar in the field of Information and Communication Engineering of Anna University, Chennai. She has more than 10 years of experience in the field of teaching. She also published papers in many International and National Conferences, Journals. He is also a member of professional bodies like IAENG, ISTE. She has guided more than 20 PG students for their project. She is interested in research on participatory sensing, wireless sensor, mobile computing, and networking.



Dr. M. Chandrasekaran is presently being the Principal of Government College of Engineering, Bargur, Tamil Nadu, India. He received the Ph.D. degree in the Department of Computer Networks from the Anna University, Chennai in 2006. He has published more than 30 Technical Papers in various Conferences and Journals. With a strong attribution towards Embedded system design and Wireless Sensor Network Research has produced 3 Ph.Ds. and supervising more than 15 Ph.D. Scholars. He has delivered numerous keynote speeches in various conferences. He served as reviewer, Technical Committee member in many conferences and Journals. Guided more than 100 UG project works and 20 PG project works. Two of the UG project works were selected for the Best Project Award by Tamil Nadu State Government in the year 1989 and 1991. Two of the UG Project works were funded by Tamil Nadu State Council for Science and Technology. One of the PG project guided by him titled "Congestion Control Algorithm for Mobile Ad Hoc Networks" got AICTE fund of Rs. 60,000/-. This Project was also selected as the Best Project. Currently serving as AICTE nominee for various Engineering Colleges and Polytechnics in Tamil Nadu for Staff Selection Committee. Member of AICTE committee for Inspecting the Infrastructure of the various Engineering Colleges in Tamil Nadu and Andra Pradesh. Member of the Inspection committee for Inspecting various Engineering Colleges and Polytechnic Colleges in Tamil Nadu by the Director of Technical Education, Chennai.