Denial of Service Attacks in Wireless Sensor Networks with Proposed Countermeasures

27

Ademola Philip Abidoye and Elisha Oketch Ochola

Abstract

A wireless sensor network (WSN) is a network consisting of small nodes with constrained capabilities to sense, collect, and transmit sensed data in many application areas such as the healthcare system, the automotive industry, sports, and open space surveillance. WSNs communicate through wireless mediums and are accessible to anyone, which makes sensor nodes vulnerable to various forms of attack. Considering the energy-constrained nature of sensor nodes, denial of service (DoS) attacks on these nodes are popular. This paper examines DoS attacks and proposes countermeasures based on use of the clustering technique. The method is compared with other related protocols, and the results show that our method is able to effectively detect and defend against DoS attacks in WSNs.

Keywords

Sensor networks · Security · Denial of service · Malicious node · Clustering · Integrity

27.1 Introduction

Recent improvement in micro-electromechanical systems (MEMs), wireless communications, highly integrated electronics, and low power devices have made the design of wireless sensor networks (WSNs) possible [1]. Sensor nodes are designed with the main aim of sensing physical quantities such as temperature, vibrations or humidity in the areas of interest. They communicate wirelessly with one another over a short distance. Generally, sensed data is transmitted from sender nodes in a hop-by-hop fashion through each intermediate node until it reaches the final destination. WSNs currently have a large range of applications and they have been successfully applied in such wide ranging applications as ubiquitous web services, structural health monitoring, and smart parking systems [2]. They can be randomly or uniformly distributed in an environment and left unattended for long periods.

However, taken together, the characteristics listed below expose sensor nodes to various security attacks, as the wireless medium is open and accessible to anyone.

- The network topology changes constantly due to the dynamic nature of the network, and damage to or the death of some sensor nodes.
- Ad-hoc deployment of sensor nodes in WSNs helps attackers to launch attacks ranging from active interference to passive eavesdropping.

This makes it important to protect WSNs against attacks and, if there is an attack, measures should be taken to ensure that its effects on the network are insignificant. Security in the context of WSNs can thus be defined as the protection of legitimate sensor nodes against all known types of attacks. These attacks can be broadly divided into active and passive attacks. Denial of service (DoS) attacks are considered mainly because they target the limited sensor node energy in a WSN. DoS attacks aim to prevent an individual sensor node from sending its reading or from communicating with the network.

In this paper, an approach called Denial of Service Attacks and Countermeasures (DOSAC) is presented as a means to detect and prevent DoS attacks in WSNs. This approach is based on the clustering technique. An algorithm is used to uniformly distribute elected cluster heads within the network.

In the next section of the paper, we discuss related work. Section 27.3 presents the proposed system design. Proposed countermeasures against DoS attacks are discussed

A. P. Abidoye (✉) · E. O. Ochola
School of Computing, University of South Africa, Johannesburg, Gauteng, South Africa
e-mail: abidoap@unisa.ac.za; ocholeo@unisa.ac.za

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_27

in Sect. 27.4. Section 27.5 presents performance evaluation, and Sect. 27.6 contains the conclusion.

27.2 Related Work

Wireless sensor nodes consist of different protocol layers of the Open Systems Interconnection (OSI) model. Each layer plays a specific role, such as framing, signalling, forwarding, reliable transportation and user interaction at both the sending as well as the receiving end. DoS attacks are identified at each layer of this model; these are purposeful, planned attacks intended to jeopardize the availability of service, thus restricting the WSN utility for application.

In [3], the authors analyse DoS attacks in WSNs. Their discussion includes the characteristics of WSNs, constraints and types of DoS attacks at different layers constituting obstacles to the smooth functioning of the networks. However, they do not provide countermeasures against the attacks.

Messai [4] divides possible attacks on WSNs into passive attacks and active attacks. The author discusses different attacks and security problems in each layer of the network's OSI model. However, he fails to provide a security measure against each attack discussed.

Han et al. [5] propose a security scheme against DoS attacks (SSAD) in cluster-based WSNs. The proposed method uses unique features to establish the trustworthiness of sensor nodes. The authors place all sensor nodes of a network into three domains: trusted, un-trusted, and uncertain. Cluster heads are selected from the trusted domain to ascertain their trustworthiness. These features allow the scheme to reduce the overhead involved in cluster head selection. In addition, it provides an efficient solution for detecting and defending against DoS attacks in a WSN.

Chen et al. [6] propose a novel method called path-based denial of service attacks (PDoS), which is operated at the base station to detect compromised sensor nodes within a network. The authors combined a Markov chain with triple exponential smoothing in order to make detection results more accurate. This approach is analytically presented; numerical representation of the model makes the approach scalable, and performance evaluation is well discussed. However, the approach is not flexible; it requires more computation, and more overhead is involved during computation.

27.3 Proposed System Design

The underlying network architecture for our proposed scheme consists of sensor nodes and a base station. With consideration for the resource-constrained nature of WSNs, we partition the network into finite clusters. Each cluster contains a cluster head (CH) and member nodes. The CHs are periodically elected from among member nodes of each cluster in order to ensure a better energy balance while maintaining best detection coverage. An approach in [7] is used to divide the network into clusters, and each node is assigned an identification number (*ID*) to uniquely identify it in the network. An algorithm in [8] is adopted in order for the CHs to be uniformly distributed within the network.

27.3.1 Analysis of Denial of Service Attacks

Traffic pattern in WSNs is many-to-one: sensor nodes deployed in a target area for environmental monitoring need to transmit their readings to a data collection centre for further processing. In-network processing such as data compression or elimination of similar readings is needed for energy efficiency. This pre-processing requires high energy level sensor nodes such as CHs to receive and aggregate the content of the sensor readings and deliver the aggregated data packets to a final destination (base station). Based on this and other characteristics of WSNs mentioned above, end-to-end data packet transmission is susceptible to DoS attacks. If packet integrity is only verified at the base station, there is a high probability that the network may forward packets injected by an attacker many hops away from source nodes to the base station before the forged messages are identified in the network. This type of attack will dissipate the energy of sensor nodes and consume network bandwidth [9].

27.3.2 Legitimate Nodes and Malicious Nodes

Legitimate nodes: Legitimate nodes are nodes whose main functionalities have not been tampered with in the network; these include normal sensor nodes, cluster heads and the base station. Legitimate nodes are susceptible to a DoS attack launched by adversarial nodes in the network.

Malicious nodes: These nodes seek to deny service to legitimate sensor nodes in the network. Malicious nodes in WSNs include the following:

(a) Compromised nodes: These are legitimate sensor nodes whose responsibilities are taken over by the attackers for the purposes of disrupting normal network operations.
(b) Injected sensor nodes: These may be either legitimate nodes with normal sensing capability, or more powerful nodes with high processing capability such as the base station [9].

Legitimate sensor nodes and malicious nodes in a network are defined as follows:

The WSN model consists of a set of sensor nodes given by $N = \{n_1, n_2, n_3, \ldots, n_V\}$; $|N| = V$ are randomly distributed

in an $M \times M$ m^2 network area. V represents the number of sensor nodes in a network.

Let $\{n_i\}$ denote set of nodes such that $1 \leq i \leq p$ denotes a set of normal nodes in a cluster $C_k \; \forall$ k = 1, 2, ...,K with k being the number of clusters, and each node n_i a legitimate sensor node in the network where $p \in \mid C_k \mid << V$.

Similarly, compromised nodes (A) in a network are expressed as follows:

$A = \left\{ n_i^{\mid} : n_1^{\mid}, n_2^{\mid}, \ldots, n_q^{\mid} \right\}$ such that $1 \leq i \leq q$, where $|A| = q \leq V$, q being the number of compromised nodes.

Thus, during network operation, legitimate nodes can transmit to themselves, to adversary nodes, and vice versa. The transmission can be expressed as follows:

1. $\mathfrak{g}(n_i: n_i \in C_k) \rightarrow \mathfrak{g}(n_j: n_j \in C_k)$; the expression shows that a normal sensor node transmits to a normal sensor node where $\mathfrak{g}$ is a routing function.
2. $\mathfrak{g}(n_i: n_i \in C_k) \rightarrow \mathfrak{g}(n_j^{\mid}: n_j^{\mid} \in A)$; the expression shows that a normal sensor node transmits to a compromised node.
3. $\mathfrak{g}(n_i^{\mid}: n_i^{\mid} \in A) \rightarrow \mathfrak{g}(n_j: n_j \in C_k)$; the expression shows that a compromised node transmits to a normal sensor node.
4. $\mathfrak{g}(n_i^{\mid}: n_i^{\mid} \in A) \rightarrow \mathfrak{g}(n_j^{\mid}: n_j^{\mid} \in A)$; the expression shows that a compromised node transmits to a compromised node.

27.3.3 DoS Attacks Detection Mechanism

It is crucial to secure all sensor readings originating from the source nodes to the destination node without the possibility of the readings being forged by adversaries. However, if an adversary is able to launch an attack, data packets can be forged and sent to a receiver node. A good algorithm should be able to detect the sender of such packets, and remove its routing path from the network so that legitimate sensor nodes will not be able to communicate with the adversary node. In addition, the receiver node should be able to drop the packets sent by the adversary. We consider attacks on WSNs from the perspective of integrity and authentication attacks, and provide countermeasures against these.

Data Integrity Attack: During data transmission, an attacker can either intercept sensor readings that are not well encrypted or break the encryption, read everything in clear text, modify the content and either play back the message over the network or drop some or all of the messages. The attacker exploits the vulnerabilities of sensor nodes to set up a zombie army (bots). Once a zombie army has been set up within the network, the attacker is ready to attack the legitimate sensor nodes and modify the encrypted data. Similarly, en route data aggregation changes the representation of original sensor readings. Thus, it becomes difficult to authenticate the correctness of aggregated data. Therefore, there is a need for a proper encryption and message integrity check algorithm to ensure that data packets received at the destination node have not been modified during transmission.

Data Authentication Attack: The intention of the attackers is to modify the content of the intercepted data packets and play back into the network. Forged and corrupted data packets could be a serious problem in a WSN, as any kind of forged data may lead to misinterpretation of a situation and be counter-productive to its own interest in military intelligence.

During communication, a sensor node relaying data packets uses its assigned code for transmission. A receiving node (CH or base station) with knowledge of the sender's personality expects a certain verification code in order to receive the packets. A man-in-the-middle adversary can perform an intercept, change the content of the sensor readings and replay the attack to pose as a sender node. This type of attack is an obstacle to the integrity of information, and deceives the receiver about the authenticity of messages from the sender.

Data integrity and authentication mechanisms are very important security measures in WSNs. The hash function is used to protect the authenticity and integrity of data packets between the sensor nodes and the base station. The hash function takes a message as input and produces an output referred to as a hash chain, or simply hash (h_C). A h_C is a set of values $\{x_0, x_1, \ldots, x_n\}$ that has length n for all $n \in \mathfrak{Z}$ such that $x_i = h(x_{i+1})$ for some hash function h, where $i \in [1, n]$ and x_0 is a valid input for h. Thus, x_n is the hash chain seed assumed to be randomly generated between 0 and 1. The length n of a hash chain is the number of hash function evaluations needed to generate the hash chain.

During network operation, the base station generates and distributes unique symmetric secret keys for all sensor nodes in the network, including the cluster heads (CHs), with the help of the elliptic curve Diffie-Hellman (ECDH) key exchange algorithm. Symmetric pre-shared keys are chosen because of low power consumption and speed compared with the asymmetric encryption technique. Individual sensor nodes receive the key and use it to encrypt their packets. A three-way-handshake connection protocol is established whenever a sensor node intends to transmit its readings to a CH node [10]. The cluster head in each cluster generates a code T_1 and sends it to a node that is given permission to transmit, while a copy of the code is kept as T_c. The code can be used to transmit only once, and it expires after 10 s. The sender node computes the hash value (H) of the message M to be transmitted, and encrypts the original message M with the shared key received from the base station. The node concatenates its ID with the encrypted M, $H(M)$ together with the code T_1 and sends it over the network to the corresponding CH for further processing.

27.4 Proposed Countermeasures AGAINST DoS Attacks

The message M in the proposed scheme can be of two types: either a legitimate message (LM) or a malicious message (MM).

Definition 1 Let LM be ξ and $\xi = \{lm_i: lm_1, lm_2, \ldots, lm_{|\xi|}\}$ and denote the set of legitimate messages which are successfully transmitted from normal nodes to the receiving node. lm_i is expressed by the tuple $lm_i = (ID, M, T_1, H)$ where ID is the unique number assigned to each sensor node, M indicates the original message, and H denotes the hash value of the message.

Definition 2 Let MM be $\wp$ and $\wp = \{mm_i: mm_1, mm_2, \ldots, mm_{|\wp|}\}$ and denote the set of messages which have been considered to be forged messages. mm_i is expressed by the tuple $mm_i = (ID, M^c, timestamp)$, where M^c indicates the content of the message that has been modified, and *timestamp* indicates the time at which M^c was considered to be a forged message.

Once a sensor node is given permission to transmit, the corresponding CH will be expecting to receive message from the node. However, if the CH was not able to receive the message from the sender node within the allocated time, it will assume the message to have been lost during transmission due to congestion. The CH will generate another code T_2, send it to the node, and update the copy of the code in its memory. During data transmission, attackers are able to intercept the concatenated message as shown in Fig. 27.1. The attackers can do two things to the message they intercept, and for each we provide a countermeasure.

27.4.1 First Layer Countermeasure

Sensor nodes communicate through a radio transceiver which is open to all neighbouring nodes, as a result of which the message transmitted during network operation is public and visible to attackers. It is possible for the attackers to know the secret key used by the sensor node to encrypt the message and to read the content of the sensor readings on the node. Alternatively, the attacker could intercept the message during transmission, modify the content, forward it to the CH and try to fool the CH into believing that the message came from a legitimate sender node. The proposed method is able to check the integrity of the message transmitted. Let us assume that an attacker is able to access and read the content on a sensor node or intercept the readings to achieve its aim during transmission. While the attacker is engaged in reading and modifying the content of the message it has intercepted, the lifetime of the code T_1 will expire. If the CH does not receive the message from the intended sender node within T_1, it generates T_2 and sends it to the node. When the CH finally receives the message, it compares the code that accompanied the message M (e.g. T_1) with stored copy T_c. If the values of T_1 and T_c are the same, then the CH will receive the message and assume that the integrity of the message M has been maintained, and that the message does indeed come from the legitimate sensor node. It is believed that an attacker cannot intercept a message, modify the content and retransmit the message within the T_1 lifetime. However, if the values of T_1 and T_c are not the same, the CH will suspect that the integrity of the message has been tampered with during transmission. It will announce the ID of the sender node to other member nodes, and mark the node as a potential attacker. A second security check is performed below in order to declare a sensor node to be an attacker.

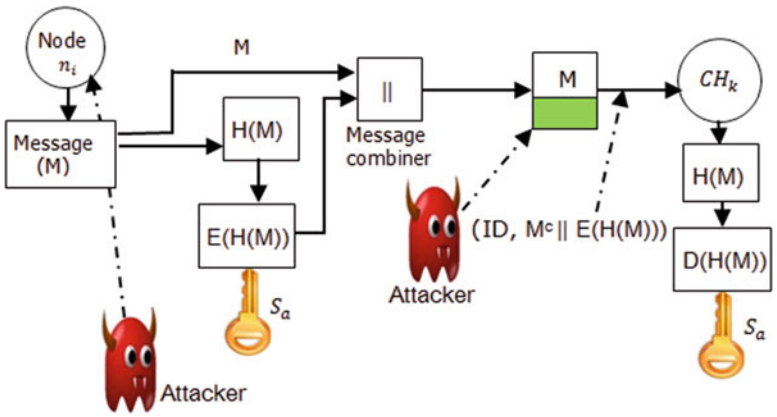

Fig. 27.1 Proposed DoS attack model

Algorithm 27.1 Malicious message detection

Begin
Given $\overline{A} = \frac{1}{|\lambda|} \sum_{i}^{new} H(M_i)$
Input $\left(M_i^{new}\right)$ and compute hash value
for $i = 1$ to $|\wp|$
if $T_1 \neq T_c$ and $D(H(M_i{}^c)) \neq E(H(M_i))$
  $\forall\, i \subseteq |\wp|$ then
  M_i are malicious messages
else
for $i = 1$ to c
  if $(M_i^{new} \subseteq |\xi|$ and $H(M_i) > \overline{A})$ then
    if $D(H(M_i)) = E(H(M_i))$ then
    M_i^{new} are legitimate messages
    end if
  end if
end if
End

27.4.2 Second Layer Countermeasure

A second layer security check is performed in order for the CH node to authenticate the integrity of the message received from the sender node. First, the CH computes the hash value of the message and decrypts the encrypted message with the copy of the shared key (S_a). Thereafter, it compares the hash value of the encrypted message M with the decrypted hash value. If the decrypted hash value of M is the same as the encrypted value, i.e. $D(H(M)) = E(H(M))$, then it will accept the message, believing that there is no attack and that the content of the message has not been modified during transmission.

Alternatively, if the hash values are not the same, i.e. $D(H(M^c)) \neq E(H(M))$, then the CH will consider that there is an attack, and that the content of the message has been intercepted and modified during transmission. It will mark the sender node as a malicious node. It forwards the details of the malicious node to the base station, which will then update the attacker node details, and compute and distribute new keys to all the nodes in the network with the exception of the attacker node. Henceforth, the attacker is blocked from communicating with other nodes in the network. Algorithm 27.1 shows pseudo code for detecting malicious nodes in a network.

27.5 Performance Evaluation

We analysed the performance of our proposed method by means of simulation, and present our results comparatively. The results shown in the graphs are the average of 35 simulations. The network consists of 100 nodes randomly distributed over a 100 m × 100 m network area. NS-2 simulator was used to evaluate the performance of the proposed scheme and compare it with other related protocols. In our simulation, the following metrics were used for performance evaluation.

Energy consumption: We performed an experiment to simulate energy dissipation in the receiving nodes. The network was attacked at 300 s and the number of messages received by the nodes exceeded 4500 during transmission. Thereafter, the proposed method was implemented to defend against the DoS attack. Energy conservation of the proposed method was greater than the result obtained without countermeasures, as shown in Fig. 27.2a.

Figure 27.2b shows scenarios with and without attackers. When the number of attackers exceeded 25%, more than 175% forged packets were sent to cluster heads. This increased the energy consumption of the cluster heads, resulting in an increase in the rate of packet loss during transmission. The proposed approach is able to effectively detect and defend against all malicious nodes and remove forged messages from the network. The packet loss rate is very low during transmission. Thus, when DOSAC is not implemented, the packet loss rate increases as the number of attackers increases. However, when the countermeasure is implemented, the number of packets transmitted from sensor nodes to their corresponding cluster heads is constant, as shown in the figure.

End-to-end delay refers to the time taken for a packet to be transmitted over a network from source node to destination. The shorter the end-to-end delay, the better the performance of the protocol. The performance of end-to-end packet delay for PDoS, SSAD and DOSAC protocols during simulation time was analysed, as shown in Fig. 27.3c. In all three protocols, packet delay increases as the number of sensor nodes increases. DOSAC has minimal end-to-end packet delay compared with SSAD and PDoS protocols because our method is able to detect malicious nodes and remove all paths emanating from them, so that legitimate nodes will not transmit through them.

Figure 27.3d shows the expected packets, as well as abnormal packet transmission delays. By periodically generating the code for sensor nodes, the cluster head is able to detect abnormal data packets. This figure shows the ability of the cluster head to identify the data integrity attack. We observe varying packet delays by monitoring the network over different time intervals. The graph shows that the cluster head identifies abnormalities when the code and hash values are not the same as its copy.

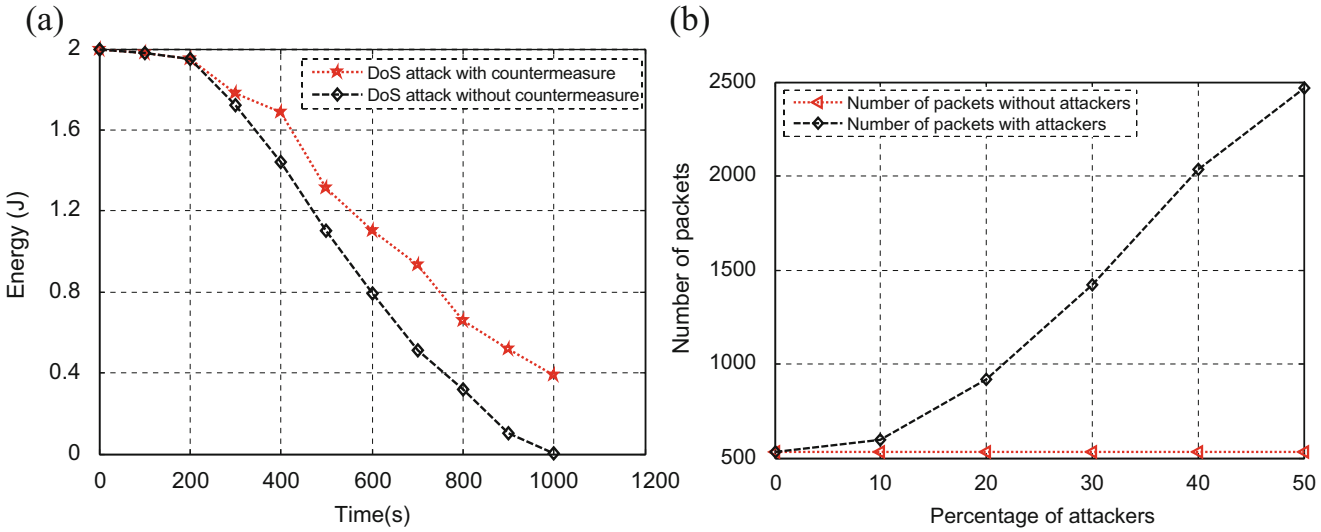

Fig. 27.2 (**a**) Energy dissipation varied with time. (**b**) Number of packets delivered versus percentage of attackers

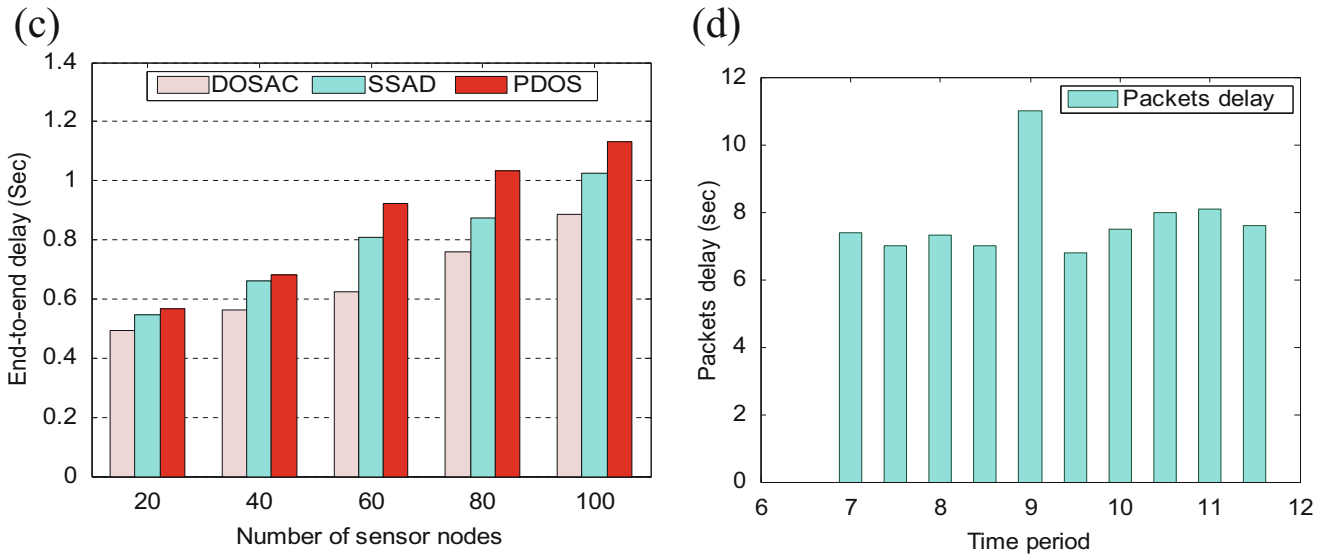

Fig. 27.3 (**c**) End-to-end delay versus number of sensor nodes. (**d**) Time period against packet delay

27.6 Conclusions

The communication patterns of sensor networks and their mode of deployment expose them to a variety of attacks. The privacy and security of data packets are the major issues of concern relating to WSNs. DoS attacks reduce the performance of the system. In this paper we present a unique method called DOSAC for detecting and defending against DoS attacks in WSNs. A hash function and encryption techniques are used to ensure data authenticity and integrity within the network. The DOSAC scheme generates unique codes and hash values to authenticate the transmission of data packets. Simulation results show that DOSAC is able to effectively detect and defend against DoS attacks in WSNs.

Acknowledgement Philip Abidoye acknowledges the support by University of South Africa, South Africa.

References

1. T. Amgoth, P.K. Jana, Energy-aware routing algorithm for wireless sensor networks. Comput. Electr. Eng. **41**, 357–367 (2015)
2. S.S. Iyengar, R.R. Brooks, *Distributed Sensor Networks: Sensor Networking and Applications*, 2nd edn. (CRC Press Taylor & Francis Group, Boca Raton, FL, 2016)
3. S. Ghildiyal, A.K. Mishra, A. Gupta, N. Garg, Analysis of Denial of Service (DOS) attacks in wireless sensor networks. IJRET. **3**, 2319–1163 (2014)
4. M.-L. Messai, Classification of attacks in wireless sensor networks, in *Proceedings of Telecommunication and Application*, (Bejaia, Algeria, 2014)

5. G. Han, W. Shen, T.Q. Duong, M. Guizani, T. Hara, A proposed security scheme against DoS attacks in cluster-based wireless sensor networks. Secur. Commun. Netw. **7**, 2542–2554 (2014)
6. D. Chen, Z. Zhang, F.-H. Tseng, H.-C. Chao, L.-D. Chou, A novel method defends against the path-based DOS for wireless sensor network. Int. J. Distrib. Sens. Netw. **2014**, 205–216 (2014)
7. G. Kannan, T.S.R. Raja, Energy efficient distributed cluster head scheduling scheme for two tiered wireless sensor network. Egypt. Inf. J. **16**, 167–174 (2015)
8. A.P. Abidoye, N.A. Azeez, A.O. Adesina, K.K. Agbele, ANCAEE: a novel clustering algorithm forenergy efficiency in wireless sensor networks. J. Wirel. Sens. Netw. **3**, 307–312 (2011)
9. C. Karlof, N. Sastry, D. Wagner, TinySec: a link layer security architecture for wireless sensor networks, in *Proceedings of the 2nd Int'l Conf. on Embedded Networked Sensor Systems*, 2004, pp. 162–175
10. W.R. Heinzelman, J. Kulik, H. Balakrishnan, Adaptive protocols for information dissemination in wireless sensor networks, in *Proceedings of ACM MobiCom'99* (Seattle, Washington USA, 1999), pp. 174–185