Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 9783072, 9 pages
http://dx.doi.org/10.1155/2016/9783072

Research Article

Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks

M. Saud Khan[1] and Noor M. Khan[2]

[1]*Department of Computer Science, Capital University of Science and Technology, Islamabad 44000, Pakistan*
[2]*Department of Electrical Engineering, Capital University of Science and Technology, Islamabad 44000, Pakistan*

Correspondence should be addressed to M. Saud Khan; saud@ciit.net.pk

Received 23 December 2015; Revised 9 May 2016; Accepted 13 July 2016

Academic Editor: Guiyun Tian

Security is always a major concern in wireless sensor networks (WSNs). Identity based attacks such as spoofing and sybil not only compromise the network but also slow down its performance. This paper proposes a low complexity sybil attack detection scheme, that is, based on signed response (SRES) authentication mechanism developed for Global System for Mobile (GSM) communications. A probabilistic model is presented which analyzes the proposed authentication mechanism for its probability of sybil attack. The paper also presents a simulation based comparative analysis of the existing sybil attack schemes with respect to the proposed scheme. It is observed that the proposed sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same sybil detection performance.

1. Overview and Related Work

Introduction. The wireless sensor networks have been widely applied in various fields in order to monitor the physical world like harvesting, battle field, habitat monitoring, and so forth. The scope of this deployment gets increased day by day due to its low cost, large scaled deployment, and self-configuration nature [1–4]. The existing designs of application for wireless sensors allow a better flexibility in terms of communication and exchange of data but are also establishing communications and increasing system automation, but also the WSNs are lacking security and privacy [3, 5, 6]. The inadequate battery life and communication and processing resources are the main limitation of a sensor node [7]. Due to these reasons, a sensor network becomes vulnerable to different threats which can lead an attacker to access secret information [8]. Sybil attack is one of the most widely launched attacks in wireless sensor networks. The sybil attack is considered very easy to be launched because of the open and broadcast nature of the wireless sensor network. In such attacks, the sybil node creates multiple identities at different locations deceiving the cluster heads (CHs) or the other nodes of the network and tries to become part of the network. The current mechanisms to detect sybil attacks are mainly based upon centralized and decentralized approaches. In centralized approach, a central entity is responsible for determining the attack and pointing out the attacking node where, as in decentralized approach, a distributed approach is used for this purpose. In [9], the authors proposed an attack detection model for sybil attacks based on RSSI. According to the authors, the model does not require any extra resources like third party or antennas and also the mobility of nodes is supported by the model. One of the implemented solutions is certification of the nodes [10]. This mechanism requires the presence of trusted and authorized third party for the validation of participating entities. The authors in [11] proposed a solution for sybil attacks based upon social networks known as sybil control which is an admission based control designed for distributed WSN. The proposed solution is basically a protocol in which a node calculates the computational work done by the other respective nodes in order to detect a malicious or misbehaving node present in the network. According to the authors, a malicious or attacking node does not have the capability to calculate the computational work of other nodes properly. Similarly, another protocol known as Gatekeeper [12] which is a decentralized admission

control protocol is also based on social network approach. Another RSSI based solution is proposed in [13]. The authors used K-means algorithm for the detection of attacking node. According to the authors, the proposed solution can also detect the location of attacking node and is enough robust to handle the variable transmission power level of attacking nodes. The RSSI based solutions are considered to be lighter in overhead since only one message is communicated but, on the other hand, RSSI being a time varying and unreliable parameter exhibits nonisotropic behavior most of the time. In [14, 15], a ranging method based approach is proposed for sybil attack detection. However, range-based algorithms involve the distance estimations by using the measurement of various physical properties of signal such as RSSI, time of arrival (TOA), and time difference of arrival (TDOA). In [16], a scheme for the detection of sybil attack is proposed on the basis of radio resource testing and registration but such approaches use high power and violate the limitation of battery power consumption. In [17, 18], the authors use Gaussian mixture model to read RSSI readings but the paper does not clearly explain how the sybil attacks are localized. In [19], the authors proposed a defense mechanism for sybil attacks based upon various resource testing like radio resource testing, position verification and registration, and so forth. In [20], a hop-by-hop authentication procedure is proposed. The authors in [21] proposed a key management mechanism that refreshes all authentication keys in order to protect them from being compromised. The authors in [22] proposed a framework, that is, performed by cluster heads in hierarchical WSN.

Problem Statement and Proposed Solution. As discussed earlier, almost every existing protocol proposed for the detection of location based attacks (like sybil attack) in sensor networks focused only on security and protection from attacks neglecting the effect of its computational complexity on the resource-constrained and bottleneck parameters like power consumption, processing capability, traffic intensity, and message latency. These parameters may lead the network towards poor performance if not handled properly. In this paper, we propose an algorithm to protect the sensor network from location based attacks like spoofing attack and sybil and so forth. The scope of this work is intentionally made limited to sybil attack in order to extend simplicity for the reader. The proposed authentication scheme is inherited from the SRES (signed response) authentication mechanism used in second-generation cellular mobile communication system, the Global System for Mobile (GSM) communication [23]. The SRES mechanism is responsible for authenticating the user and encrypting the voice data. In order to implement the SRES in WSNs, we modified the original scheme to fit it into ad hoc scenario. Simulations are performed to validate the performance of the proposed algorithm in MATLAB®. From the simulation results, we prove that the proposed scheme not only is enough efficient to detect the sybil attack but also requires lesser processing and battery power as compared to notable existing authentication schemes. Moreover, the scheme creates little message overhead resulting in negligible increase in the traffic of the network. In order to prove the efficiency, comparison of the proposed algorithm is carried out with two notable attack detection and authentication schemes, that is, Detecting and Locating Location Based Attack Detection (LBAD) in wireless sensor networks [13] and Lightweight Sybil Attack Detection (LwSAD) in MANETs [9]. Both the schemes are evaluated over probability, processing overhead, and power consumption.

The rest of the paper is organized as follows.

Section 2 explains the procedure of authentication in GSM technology. Section 3 discusses the proposed attack model and defense strategy, respectively. The simulation results and performance comparison are discussed in Section 4 followed by conclusions in Section 5.

2. Working of Authentication Algorithms in GSM

The signed response procedure is originally designed for second-generation GSM based networks. This mechanism is responsible for handset authentication to the network. The A3 algorithm is used to produce a response against the challenge (SRES) as elaborated in Figure 1. The Subscriber Identity Module (SIM) also contains the ciphering key generating algorithm (A8 algorithm). The A8 algorithm is used to calculate the 64-bit ciphering key (K_c) which is used to encrypt the voice data before it is sent over the channel. The ciphering algorithm A5 is used to authenticate and ensure the secure communication between the mobile station (MS) and the network. The GSM network initiates a request and sends to mobile station over the channel. The A3 algorithm which is embedded in the handset is responsible for generating the signed response (SRES). The block diagram of A3 algorithm is shown in Figure 2 which involves the process of creating a 32-bit signed response from 128-bit key (RAND). The detailed step-by-step procedure of mobile authentication and voice encryption in GSM is given below:

(1) The mobile station (MS) initiates process to sign in to the network.

(2) A request for 5 triples to Mobile Services Switching Center (MSC) is forwarded from the Home Location Register (HLR).

(3) With the help of A8 algorithm, the five triples are created by Home Location Register and sent to MSC comprising the following main components:

  (i) 128-bit random challenge (RAND).
  (ii) 32-bit matching SRES.
  (iii) 64-bit ciphering key used as a Session Key (K_c).

(4) From the first triple, a random challenge is sent to Base Transceiver Station (BTS) from the Mobile Services Switching Center. The BTS then forwards the challenge to mobile station.

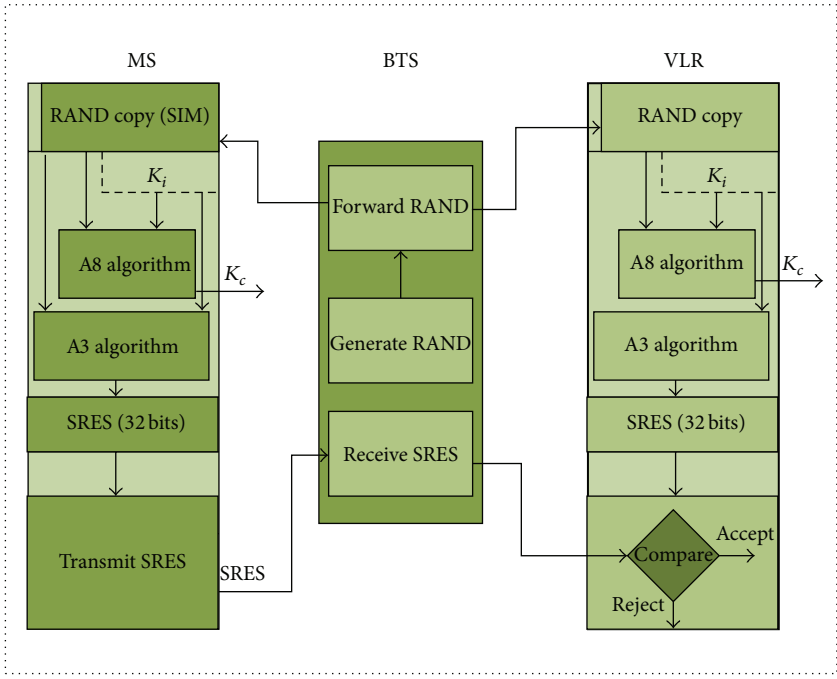


Figure 1: Authentication process in GSM.

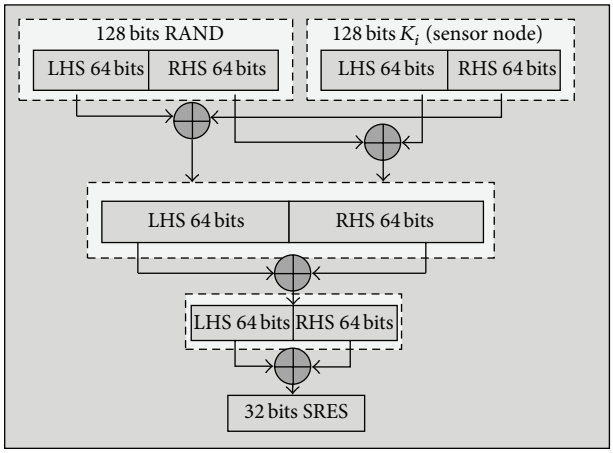


Figure 2: Block diagram of A3 algorithm generating 32-bit SRES.

(5) After receiving the challenge from BTS, the mobile station starts the process of encryption with authentication key K_i assigned to it. The encryption process is carried out with the help of A3 algorithm.

(6) Mobile station creates a SRES and sends to the BTS.

(7) The Base Transceiver Station forwards the SRES to the Mobile Services Switching Center.

(8) The SRES is verified by Mobile Services Switching Center.

The use of A8 algorithm for session creation by a mobile station is not discussed in this section since it does not come in our scope.

3. Low Complexity Signed Response Based Sybil Attack Detection Mechanism

3.1. Network Model and Assumptions. Figure 3 illustrates a distributed network with hierarchical structure having cluster heads (CHs) along with the member sensor nodes. We assume that the CH is a powerful node that may become a sink in case of a centralized network. The sybil nodes S are assumed to be present in the network and they have the complete information of security mechanism of the network. The CH is responsible for monitoring the behavior of sensor nodes in its vicinity and ensuring that there is no attacker or sybil node. The CH sends the attack information to the BS or any controlling entity if determined. Although only one BS is shown in Figure 3 but there could be as many BS as required by the network and environment. The deployment of nodes can be aerial or manual depending upon the nature of physical environment. Each sensor node is assigned an ID and the position of the sensor node is assumed to be known to it. We also assume that the sink or cluster head has all the necessary information about member sensor nodes like sensor ID, sensor MAC address, and the assigned authentication key K_i.

3.2. Proposed Methodology. In order to implement the SRES mechanism in WSN, we make necessary modifications in the existing authentication scheme implemented in GSM. The proposed mechanism can also be used both in centralized and in clustered ad hoc environment. In ad hoc mode, a sink is responsible for coordinating with all the nodes in the network whereas, in clustered mode, a cluster head can authenticate the node. Since data encryption is not covered in this paper,

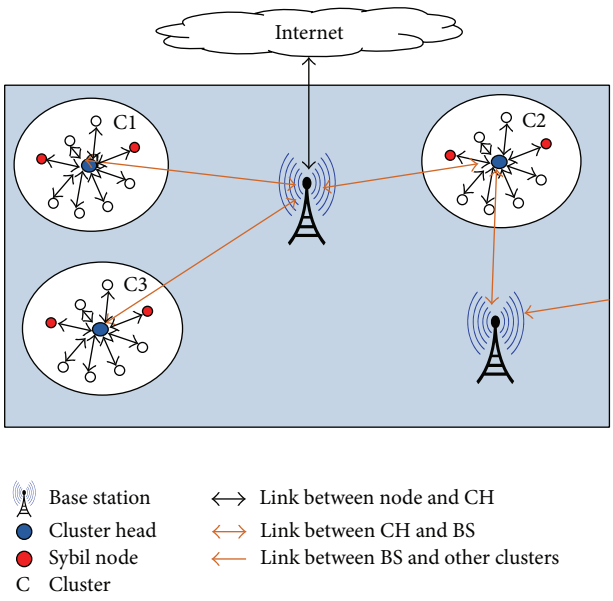


FIGURE 3: An overview of sensor network with sybil nodes.

we will not use the voice encryption algorithm which is also part of the GSM security module. The step-by-step procedure of the proposed algorithm is given below:

(1) The five triples are generated and provided by the server or cluster head (CH) or sink side. The five triples are comprised of the following:

(i) 128-bit random challenge (RAND).
(ii) 32-bit matching SRES.
(iii) 64-bit ciphering key used as a Session Key (K_c).

(2) RAND is forwarded to the sensor nodes as a challenge in order to authenticate it.

(3) This challenge can be sent either as a broadcast if all the nodes need to be authenticated through single challenge number or as a unicast if a specific node is meant to be authenticated.

(4) Every node has a MAC address and is also provided a preshared key K_i. Thus, a node can produce the SRES with either MAC address or K_i depending upon the implementation.

(5) The signed response (SRES) can be sent by the node directly to either a server, CH, or SN depending upon the nature of the wireless sensor network.

(6) The server, CH, or sink verifies the SRES sent by the node and acts accordingly (allowing or disallowing the node).

Figure 4 shows the block diagram of proposed authentication scheme where a sink generates and forwards a challenge to the node(s). The MAC address of each node that can be considered as K_i is required to be registered with the sink or CH. The GSM does not allow a mobile station to authenticate the network. However, in our proposed scheme, we will use the SRES to authenticate the network by each member node of the network. In order to verify the network, a node N can request the sink or cluster head to resend its already sent SRES to it for confirmation. It means that a node can verify whether it is communicating with the right and authentic network or not. However, this verification can be carried out after a certain number of SRESs have already been generated by the node N. As an extension of this work in the future, we will enable the node to reverse the authentication process without sending any challenge to the network.

3.3. Attack Model and Defense Strategy. In order to launch the attacks and test the efficiency of the proposed scheme, we establish a network of 1000 sensor nodes deployed randomly in an arbitrary area. It is assumed that each node is able to communicate with at least one neighboring node in the network. Since the proposed scheme can work both in centralized and in hierarchical networks, we take both structures on board in our simulations while launching attack and executing defense mechanism. The sybil node present in the network is assumed to be a powerful node with respect to both processing and battery power. A sybil node cannot be registered to the network until it successfully verifies itself as a member sensor node of the network to either the server, CH, or SN. To become a member of the network, the sybil node launches repeated attacks in two ways; it either generates and sends the fake IDs to the respective SN or CH or attempts to steal the ID of a valid member sensor node from the network. If the sybil node with a fake ID achieves success in participating in the network without being identified, we will call it a valid sybil identity. In order to make the situation harder for a sybil node, we will perform validation test. There are two types of validations, direct validation and indirect validation. In direct validation, a node can directly check whether the node in its neighborhood or vicinity is having a valid identity or not based upon the knowledge it possesses. In indirect validation, different nodes can communicate during validating a targeted node so that a globally consistent decision can be made. The indirect validation mechanism is considered to be costly as compared to direct validation because, in the latter case, if a node A having an identity ID_i tries to validate an identity ID_j of a node B, the massages need to be exchanged only between nodes A and B via a single hop, whereas, in the former case, other nodes of the network have to be taken on board for an identity validation. In order to prove the efficiency of the proposed authentication protocol, we evaluate it on both direct and indirect validation processes. To verify a node and its identity in the network through direct validation, the verifier (CH or SN) challenges the identity by sending challenge to the targeted node laying in its one-hop neighborhood. The challenge in our case is a 128-bit random number generated by authenticating party, that is, the server or CH or SN. Upon the reception of challenge number, the targeted node will encrypt it with either its MAC address or K_i with the help of A3 algorithm to generate the SRES. At the same time the authenticating party also calculates the SRES from the random number sent and the same K_i from the database as with the targeted node.

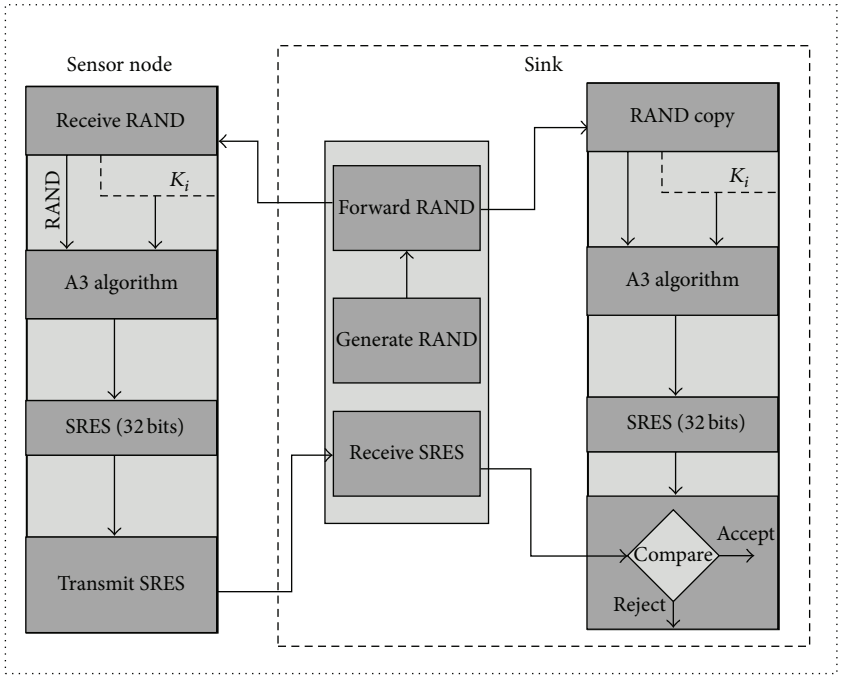


Figure 4: Block diagram of the proposed authentication scheme for wireless sensor networks.

When the authenticating party receives the SRES from the targeted node, both the values of SRES are compared. These values must be the same if the node is a valid one; otherwise it will be declared as sybil node. In case of indirect validation, the authenticating node N sends a challenge to a targeted node T which is not in its one-hop neighborhood N. Thus, this challenge has to reach the targeted node in a hop-by-hop manner. Upon the reception of the challenge, the node T will calculate the SRES through A3 algorithm and sends back to node N. The process of calculating the SRES is the same as discussed for direct validation.

The steps involved in the proposed authentication scheme are represented in Algorithm 1. Line (1) generates five vectors of sizes 32, 64, 128, 256, and 512. Note that each value of table T_i ranges from 0 to 2^{4+j-1}, where $j = 1, 2, 5$. In line (4) the sybil node generates and forwards the SRES to the authenticating party through $\Psi_a(T, R_k, \Psi_{r,16}$ (0 to $2^8 - 1))$ whereas the authenticating party validate the SRES received from attacking node through $\Psi_a(T, R_k, K_{i,j}$, where $j = 1$ to Pool Size). Similarly lines (10)–(23) show the step-by-step process of $X \oplus R$ by dividing the RAND and K_i into LHS and RHS to produce the 32-bit SRES.

4. Probabilistic Model of the Proposed Scheme

let the key size be α, and let the pool size in the sink be β.

Consider K_i, where $(1 \leq i \leq n)$ is the predistributed ith key from a vector space $K = K_1, K_2, K_3, \ldots, K_n$ of size $n = 2^\alpha$. If the sybil node generates a random key K_a, then the probability of this key being a valid key is

$$P(K_a) = P(K_i) = \frac{1}{|K|}, \tag{1}$$

where $|K|$ is the cardinality of the vector space K. Since $|K| = n$ therefore

$$P(K_i) = \frac{1}{2^\alpha}. \tag{2}$$

This gives us the probability of a randomly generated key to be accepted by the sink. let us suppose that a node uses a pool size of β of predistributed keys, and then S is the subspace of predistributed keys in the pool such that $S \subseteq K$, where $S = \{S_i \in K \mid 1 \leq i \leq \beta\}$. Now, with the probability of any key S_i being in the subspace S, $P(S_i)$ becomes

$$P(S_i) = \beta P(K_i). \tag{3}$$

Probability that a key S_a is being attacked by the sybil node from the pool of β keys is

$$\text{Prob}(S_a) = P(S_i) = P. \tag{4}$$

Suppose that we have M number of sybil nodes attacking on a network. The probability that j attacking sybil nodes are successful out of M nodes is given as

$$\begin{aligned}
&\text{Prob}(j \text{ sybil nodes are successful out of } M \text{ nodes}) \\
&= \binom{M}{j} P^j (1 - P)^{M-j} \\
&= \binom{M}{j} [\beta P(k_i)]^j [1 - \beta P(k_i)]^{M-j} \\
&= \binom{M}{j} \beta^j \frac{1}{2^{\alpha j}} \left[1 - \frac{\beta}{2^\alpha}\right]^{M-j}
\end{aligned}$$

(1) $T_{i,1:2^{4+i}} \leftarrow \Psi_r(0 \text{ to } 2^{(4+i-1)} - 1)$, $i \in \{1, 2, 3, 4, 5\}$
(2) {Sybel attack}
(3) **for** 1 to number of attacks **do**
(4) **if** $\Psi_a(T, R_k, \Psi_{r,16}(0 \textbf{ to } 2^8 - 1)) = \Psi_a(T, R_k, K_{i,j}$, where $j = 1$ to Pool Size) **then**
(5) useble sybil
(6) **else**
(7) sybel detected
(8) **end if**
(9) **end for**
(10) SRES = $\Psi_a(T, R_k, K_i)$
(11) **for** $i \leftarrow 1$ **to** 8 **do**
(12) $X_{1:16} \leftarrow K_i$
(13) **for** $j \leftarrow 1$ **to** 5 **do**
(14) **for** $l \leftarrow 1$ **to** $25 - j$ **do**
(15) $m \leftarrow l$
(16) $n \leftarrow m + 25 - j$
(17) $y \leftarrow ((X_m + 2 * X_n) \text{mod} 29 - j) + 1$
(18) $z \leftarrow ((2 * X_m + X_n) \text{mod} 29 - j) + 1$
(19) $X_m \leftarrow T_{j,y}$
(20) $X_n \leftarrow T_{j,z}$
(21) **end for**
(22) **end for**
(23) **end for**
(24) Convert X to corresponding binary key B
(25) Permute B
(26) SRES $\leftarrow B_{1:32}$

Algorithm 1: Algorithm of the proposed authentication scheme.

$$= \binom{M}{j} \frac{\beta^j}{2^{\alpha} j} \left[\frac{2^{\alpha} - \beta}{2^{\alpha(m-j)}}\right]^{(M-j)}$$

$$= \binom{M}{j} \frac{\beta^j \left(2^{\alpha} - \beta\right)^{M-j}}{2^{\alpha j} \cdot 2^{\alpha M} \cdot 2^{-\alpha j}} = \binom{M}{j} \frac{\beta^j \left(2^{\alpha} - \beta\right)^{M-j}}{2^{\alpha M}}. \tag{5}$$

Therefore, probability of total successful sybil attacks if M nodes attack the network is given as

$$P_{\max} = \sum_{j=1}^{M} \binom{M}{j} \frac{\beta^j}{2^{\alpha M}} \left(2^{\alpha} - \beta\right)^{M-j}. \tag{6}$$

Figure 5 shows the probability that at least one sybil node is successful out of M attacking sybil nodes in the proposed sybil prevention scheme. Moreover, Figure 6 shows the maximum probability when one or more attacking sybil nodes become successful under different sizes of authentication key. This figure shows a sharp exponentially declining trend in the probability as the number of useful sybil nodes increases.

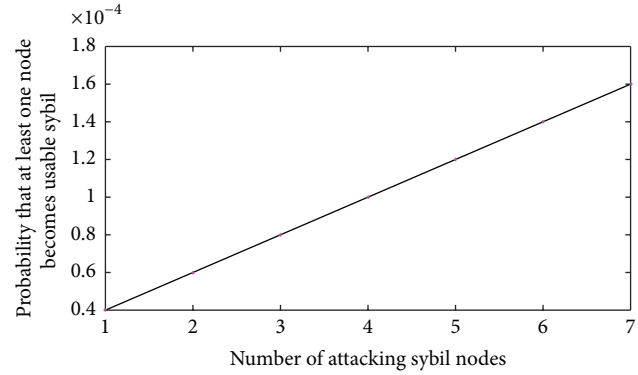


Figure 5: Successful probability of at least one sybil node in a pool of M sybil nodes.

5. Results and Discussion

In this section, we discuss the simulation results and provide a detailed performance analysis of the proposed scheme. As discussed earlier, the simulations are based on a network of 1000 sensor nodes. The parameters that we consider for performance are probability of usable sybil, traffic behavior, power consumption, and probability of attack detection.

5.1. Probability of Usable Sybils. The capability of a security algorithm can be better judged on the basis of its probability of letting sybil nodes successfully utilize the network. Figure 7 shows the probability of successful sybil attacks as exhibited by the proposed and referenced mechanisms. If a sybil node is successfully injected to the network without being detected, we call it usable attack. The attacks are launched and tested with the pool sizes of $N_{K_c} = 1$ and $N_{K_c} = 2$. The case of $N_{K_c} = 2$ is even more harder for sybil node to get through as compared to $N_{K_c} = 1$. However, the earlier case requires relatively more processing overhead than the latter one. The result shows that the proposed scheme provides a better protection

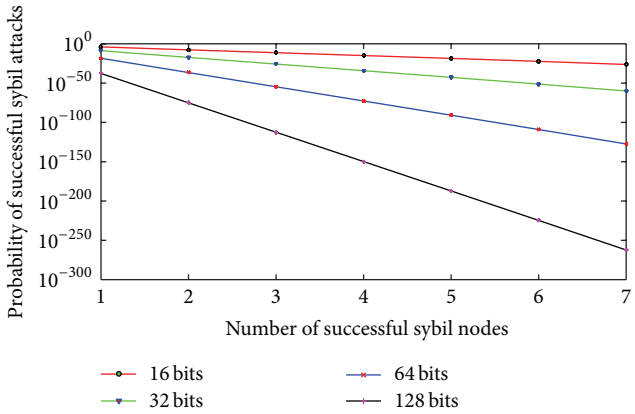


Figure 6: Probability of successful attacks by sybil nodes.

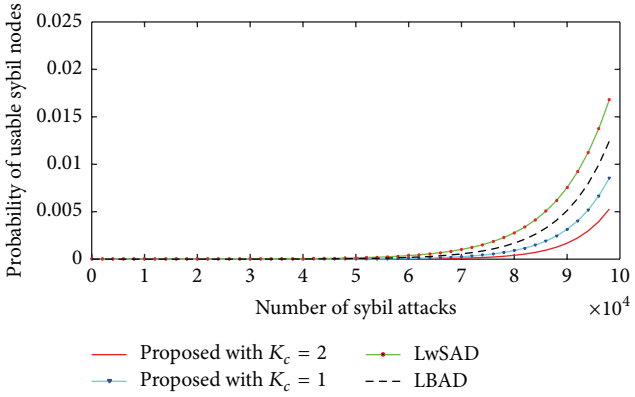


Figure 7: Probability that a sybil node will go undetected by the various algorithms.

since the probability of usable sybil node is lower in both cases ($N_{K_c} = 1$ and $N_{K_c} = 2$) than the LBAD and LwSAD.

5.2. Traffic Analysis. The lifetime of a wireless sensor network is directly proportional to the rate of exchange of packets. Excessive amount of packet exchange leads to a rapid battery drain due to which the network may die out. Figure 8 shows the behavior of algorithms against the traffic of the network during authentication process. It can be observed from the figure that the proposed scheme produces lesser number of packets in both cases of $N_{K_c} = 1$ and $N_{K_c} = 2$ as compared to LBAD and LwSAD. The number of packets generated is also directly proportional to the number of authentication rounds launched by a node or CH and will thus be borne at the cost of enhanced security of the network. This result also verifies our claim that the proposed scheme consumes lesser processing power and does not adversely affect the network lifetime.

The little overhead produced as a result of exchange of packets regarding authentication of the nodes can be borne at the cost of secure network. The traffic overhead is directly proportional to the number of authentication procedures launched by CH or SN depending upon the network.

5.3. Node Power Consumption. While designing a protocol for sensor nodes, the power consumption should always

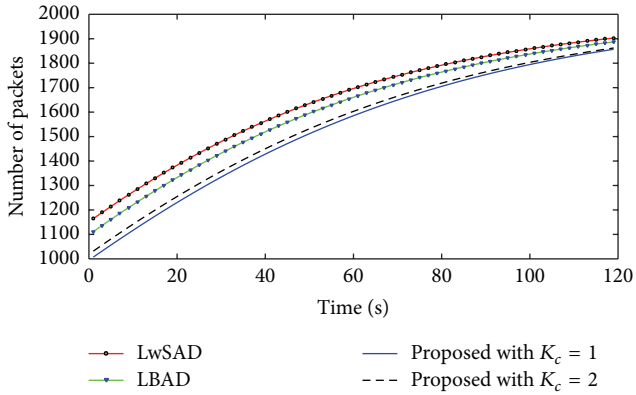


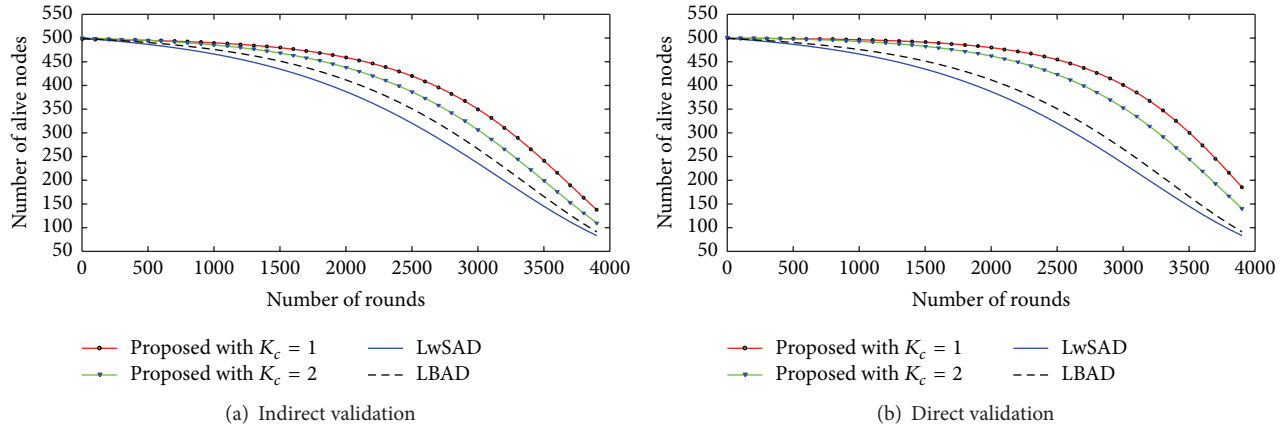
Figure 8: Simulated traffic behavior of the WSN while executing the proposed and existing authentication schemes.

be taken on board especially when the network has no resource of additional power supply once deployed. The power consumption of nodes is also calculated in case of direct and indirect validation of the nodes. As already discussed, the indirect validation requires more processing and communication power as compared to direct validation. Figures 9(a) and 9(b) illustrate the results of simulation with respect to power consumption in both direct and indirect validation process against authentication rounds. The graph shows the combined power consumption of all nodes either at both ends of the communication link or at the intermediate nodes during the process of authentication of a node or a set of nodes. The proposed authentication protocol consumes much lesser power in indirect validation as compared to direct validation as shown in Figures 9(a) and 9(b). The power consumption in case of indirect validation is due to information exchange like challenge and SRES between the originating and destination sensor nodes. This operation engages all the nodes that come in the path. Power consumption in case of indirect validation thus depends significantly on nodes population. Larger networks will consume more power in indirect validation and vice versa.

5.4. Probability of Attack Detection. Probability of attack detection is a major parametric criterion to evaluate the performance of a security algorithm. Figure 10 represents the probability of detection shown by each algorithm applied to the network. It can be clearly seen that the proposed algorithm provides a better protection against the sybil attacks. If we increase the pool size of keys in the sensor nodes, the situation will become even harder for the sybil node. However, this may demand more memory and processing capability available at each sensor node. Therefor, we limited the size up to $N_{K_c} = 2$. The pool size thus is subject to the requirement of the desired security level, power availability at the sensor nodes, and number of nodes in the network.

6. Conclusion

The existing approaches of defense against the sybil attacks are becoming incapable day by day due to increase in the



(a) Indirect validation

(b) Direct validation

FIGURE 9: Power consumption and remaining number of alive nodes as a result of power consumption by participating nodes during the process of authentication in various algorithms.

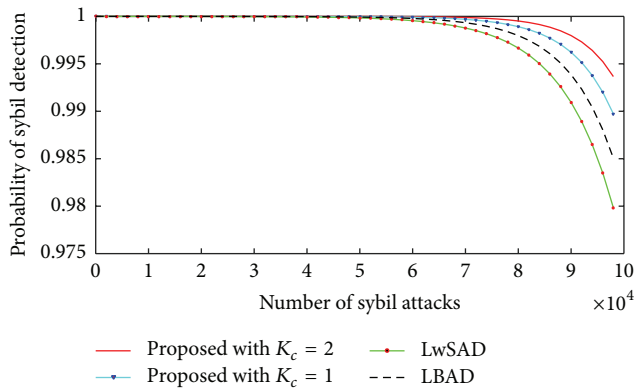


FIGURE 10: Probability of sybil node detection by the proposed algorithm in comparison with the existing algorithms.

processing power and capability of attacking nodes. A sybil node can now launch thousands of attacks before its battery gets drained or its processing capability is exhausted. In this paper, we have proposed a low complexity sybil attack detection mechanism which is based on the SRES authentication mechanism developed for Global System for Mobile (GSM) communications. The SRES mechanism is responsible for authenticating the user and encrypting the voice data. The proposed scheme can be implemented in both hierarchical and centralized wireless sensor networks. The proposed scheme has been analyzed for its performance under various sybil attacks. The scheme has been evaluated for its probability of detecting sybil nodes when different authentication key pool sizes are utilized. After extensive simulations, it has also been observed that the proposed scheme is able to detect sybil attacks with higher probability as compared to existing state-of-the-art existing schemes. It has been observed that the proposed sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same sybil detection performance.

Competing Interests

The authors declare that they have no competing interests.

References

[1] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xi, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 22–35, 2015.

[2] M. Winkler, M. Street, K.-D. Tuchs, and K. Wrona, "Wireless sensor networks for military purposes," in *Autonomous Sensor Networks*, D. Filippini, Ed., vol. 13 of *Springer Series on Chemical Sensors and Biosensors*, pp. 365–394, Springer, Berlin, Germany, 2013.

[3] D. Sun, X. Huang, Y. Liu, and H. Zhong, "Predictable energy aware routing based on dynamic game theory in wireless sensor networks," *Computers & Electrical Engineering*, vol. 39, no. 6, pp. 1601–1608, 2013.

[4] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.

[5] I. Bekmezci and F. Alagaz, "Energy efficient, delay sensitive, fault tolerant wireless sensor network for military monitoring," *International Journal of Distributed Sensor Networks*, vol. 5, no. 6, pp. 729–747, 2009.

[6] X. Xu, "Sequential anomaly detection based on temporal-difference learning: principles, models and case studies," *Applied Soft Computing Journal*, vol. 10, no. 3, pp. 859–867, 2010.

[7] N. Aslam, W. Phillips, W. Robertson, and S. Sivakumar, "A multi-criterion optimization technique for energy efficient cluster formation in wireless sensor networks," *Information Fusion*, vol. 12, no. 3, pp. 202–212, 2011.

[8] P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, and L. Buttyán, "Secure and reliable clustering in wireless sensor networks: a critical survey," *Computer Networks*, vol. 56, no. 11, pp. 2726–2741, 2012.

[9] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in MANETs," *IEEE Systems Journal*, vol. 7, no. 2, pp. 236–248, 2013.

[10] B. Viswanath, M. Mondal, A. Clement et al., "Exploring the design space of social network-based Sybil defenses," in *Proceedings of the 4th International Conference on Communication Systems and Networks (COMSNETS '12)*, pp. 1–8, Bangalore, India, January 2012.

[11] F. Li, P. Mittal, M. Caesar, and N. Borisov, "SybilControl: practical sybil defense with computational puzzles," in *Proceedings*

of the 7th ACM Workshop on Scalable Trusted Computing (STC '12), pp. 67–78, October 2012.

[12] N. Tran, J. Li, L. Subramanian, and S. S. M. Chow, "Optimal Sybil-resilient node admission control," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM '11)*, pp. 3218–3226, Shanghai, China, April 2011.

[13] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2418–2434, 2010.

[14] J. Yang and Y. Chen, "A theoretical analysis of wireless localization using RF-based fingerprint matching," in *Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS '08)*, pp. 1–6, Miami, Fla, USA, April 2008.

[15] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proceedings of the International Symposium on on World of Wireless, Mobile and Multimedia Networks (WOWMOM '06)*, pp. 564–570, IEEE Computer Society, Buffalo, NY, USA, June 2006.

[16] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM Workshop on Wireless Security (WiSe '06)*, pp. 43–52, New York, NY, USA, 2006.

[17] A. Wool, "Lightweight key management for IEEE 802.11 wireless LANs with key refresh and host revocation," *Wireless Networks*, vol. 11, no. 6, pp. 677–686, 2005.

[18] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, 2005.

[19] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN '04)*, pp. 259–268, ACM, Berkeley, Calif, USA, April 2004.

[20] M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in *Proceedings of the 2nd ACM Workshop on Wireless Security (WiSe '03)*, pp. 79–87, ACM, San Diego, Calif, USA, September 2003.

[21] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks," in *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW '03)*, pp. 749–755, Providence, RI, USA, May 2003.

[22] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00)*, vol. 2, pp. 775–784, IEEE, March 2000.

[23] M. Y. Rhee, *Mobile Communication Systems and Security*, John Wiley & Sons, New York, NY, USA, 2009.