IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 13, 2020, accepted February 27, 2020, date of publication March 4, 2020, date of current version March 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2978303

MAC-AODV Based Mutual Authentication Scheme for Constraint Oriented Networks

MUHAMMAD ADIL[1], RAHIM KHAN[2], MOHAMMED AMIN ALMAIAH[3], MOHAMMED AL-ZAHRANI[4], MUHAMMAD ZAKARYA[2], MUHAMMAD SAEED AMJAD[1], AND REHAN AHMED[1]

[1]Department of Computer Science, Virtual University of Pakistan, Lahore 23200, Pakistan
[2]Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan
[3]Department of Computer and Information Science, King Faisal University, Al-Ahsa 00966, Saudi Arabia
[4]College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 00966, Saudi Arabia

Corresponding author: Rahim Khan (rahimkhan@awkum.edu.pk)

This work was supported by the Deanship of Scientific Research at King Faisal University under Grant 187113.

ABSTRACT Wireless sensor networks (WSNs) is an infrastructure free organization of various operational devices. Due to their overwhelming characteristics, these networks are used in different applications. For WSNs, it is necessary to collect real time and precise data as critical decisions are based on these readings in different application scenarios. In WSNs, authentication of the operational devices is one the challenge issue to the research community as these networks are dynamic and self-organizing in nature. Moreover, due to the constraint oriented nature of these devices a generalized light-weight authentication scheme is needed to be developed. In this paper, a light-weight anonymous authentication techniques is presented to resolve the black-hole attack issue associated with WSNs. In this scheme, Medium Access Control (Mac) address is used to register every node in WSNs with its nearest cluster head (CH) or base station module(s). The registration process is performed in an off-line phase to ensure authenticity of both legitimate nodes and base stations in an operational network. The proposed technique resolves the black-hole attack issue as an intruder node needs to be registered with both gateway and neighbouring nodes which is not possible. Moreover, a hybrid data encryption scheme, elliptic curve integrated encryption standard (ECIES) and elliptic curve deffi-hellman problem (ECDDHP), is used to improve authenticity, confidentiality and integrity of the collected data. Simulation results show the exceptional performance of the proposed scheme against field proven techniques in terms of minimum possible end-to-end delay & communication cost, maximum average packet delivery ratio and throughput in presence of malicious node(s).

INDEX TERMS WSNs, AODV protocol, black hole attacks, MAC-Based AODV, authentication.

I. INTRODUCTION

Wireless sensor networks (WSNs) play a vital role in automating and upgrading different parts of our daily life activities such as patients diagnosis, smart homes or offices, parking, safety and security measures etc. Sensors embedded devices, i.e., sensor boards, are deployed to collect real time data such as detection of movable objects in smart homes application or pulse count in health care or intruder detection in military application [1], [2]. Generally in WSNs, data collected by sensor boards, which consists of confidential and sensitive information, is transmitted to a central location, i.e., gateway or server, through either direct or multi-hop communication mechanism [3]. This sensitive data needs to be collected and accessed solely by authenticated device(s) in an operational network. Authentication of operational devices in WSNs is a primitive process which is used to verify the identity of both sender and receiver modules. Before initiation of the actual communication process, any board or device interested in sharing of information must prove its identify, i.e., it is an authentic node, to the receiving device and vice versa [4]. Usually in WSNs, Sensor boards or devices are limited in terms of processing, communication, power and sensing capabilities. Therefore, for these networks, authentication process is needed to light-weight and efficient particularly in terms of processing and power consumption to

The associate editor coordinating the review of this manuscript and approving it for publication was Kaiping Xue.

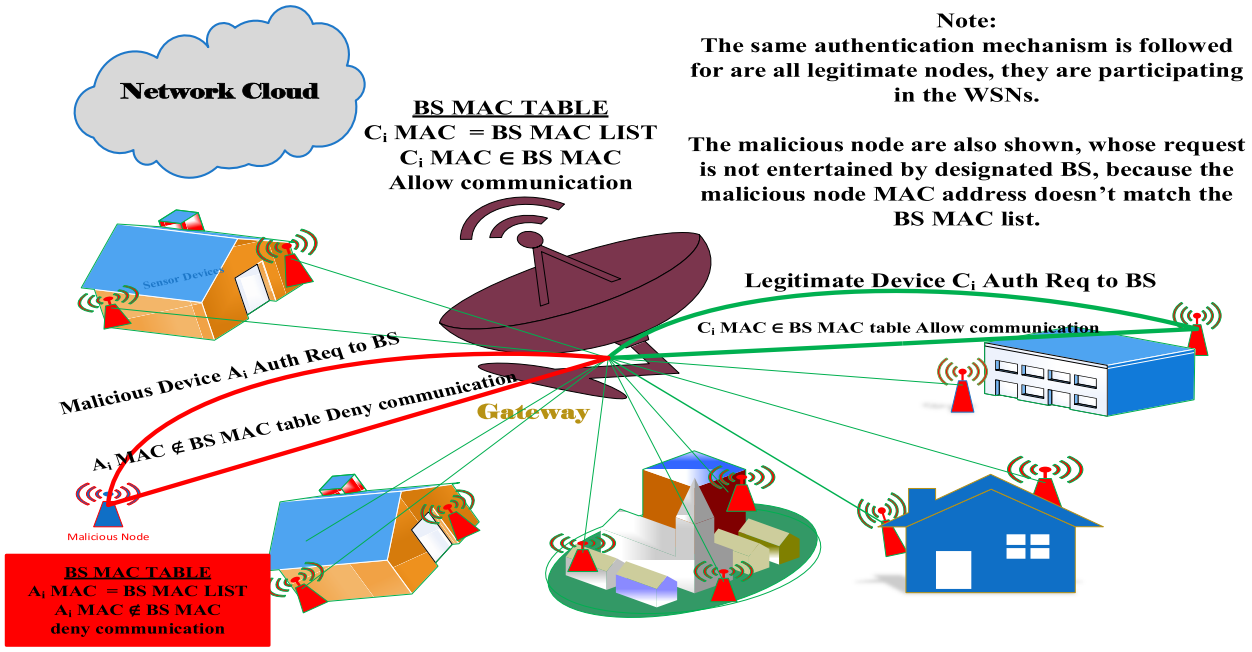

FIGURE 1. Request initiation process of both legitimate and intruder node with the concerned base station in an Operational network.

avoid or prevent various attacks such as black-hole, man-in-middle and reply etc [5].

In literature, various authentication schemes have been proposed to secure the collected data by ensuring devices authenticity prior to the initialization of the transmission process i.e., actual data transmission [6]–[8]. Although, these techniques have resolved the security problem associated with constraint oriented networks, they incur a comparatively higher computational and communication cost. The complexity of an authentication scheme has a direct correlation with the performance of an operational network in general and WSN in particular. Usually, existing techniques have utilized various cryptosystems, i.e., symmetric, asymmetric and hybrid systems, to guarantee authenticity, integrity and confidentiality of both data and devices [9]. Point-to-point authentication among nodes of an operational constraint oriented network is achieved through extensible authentication protocols, P2P, IPsec and host identity mechanism [10]–[13]. Likewise, trust based authentication and extended ad-hoc on demand distance vector (EAODV) were presented to address the black-hole attack issue associated with the constraint oriented networks [14]. Moreover, a two tier approach is proposed in literature to address this issue particularly the black-hole attack problem [15]. Although, these techniques perform exceptionally well in resolving the authenticity and confidentiality issues, but have compromised either on the complexity of the schemes or authenticity of the operational devices or both. These compromises lead to the black-hole attack in constraint oriented networks. For example in both AODV and EAODV authentication schemes, a malicious node is able to deceive a neighbouring node or gateway or both.

In this paper, a light-weight mutual authentication scheme for WSNs is presented to address the authenticity and confidentiality issues associated with an operational network particularly WSNs and IoTs. The proposed scheme is not only reliable in terms of the operational devices' authenticity issue, but it is also computationally efficient as described in the results section. A detailed description of the proposed MAC based registration process is depicted in Figure. 1 where both scenarios were presented i.e., a legitimate node C_i and intruder node A_k request and response process with the concerned base station S_j. In figure 1, green lines represent the communication between legitimate nodes and BS whereas red lines are used to describe request initiation process of the malicious node(s) with the nearest BS.

The main contributions of this research work, particularly from WSNs' perspective, are described below.

1) A hybrid device authentication and communication algorithm
2) A node C_i is Authentic **iff** its MAC address is registered with the concerned BS.
3) Avoidance measures for the black-hole attack through MAC address registration scheme in off-line phase.
4) A hybrid data encryption scheme for the resource limited devices to improve integrity and reliability of the collected or transmitted data.
5) The proposed approach uses minimum (possible) number of XOR operations and hash functions.
6) Various claims of the proposed approach is justified with appropriate simulation measures.

The remaining paper is organized as follows. In subsequent sections II, an overview of the literature, preferably closely linked to the problem addressed such as black-hole

attacks, is presented. In section III, a detail description of the proposed methodology with mathematical modelling is presented. In subsequent section, an informal security analysis of the proposed scheme is presented. In section V, various simulation parameters and results are discussed in detail. Finally, concluding remarks are given.

II. LITERATURE REVIEW

Authentication of devices in an operational network is a challenging issue for the research community in general and networks of resource limited devices in particular [16]. As these networks, i.e., WSNs and Internet of things (IoTs), have limited processing and transmission powers subjected to the devices' infrastructure i.e., processors and Xbee modules [17]. Hence, authentication scheme(s) for these constraints oriented networks must be light-weight in terms of excessive processing and communication overheads. Moreover, authentication scheme(s) need to resolve or prevent majority of the possible threats or attacks such as black-hole, jamming, tempering, and Sybil etc.

To address the authentication issue, various techniques have been presented in literature. A complete review of those mechanisms is beyond the scope of this paper, therefore, a comprehensive review of existing methodologies which are closely linked to the proposed approach is presented. Initially, AODV based methods were used to secure the constraint oriented networks against the aforementioned attacks particularly black-hole [18], [19]. These protocols have ensured the loop free structure of the operational networks, i.e., WSNs and IoTs, with proper routes management system through a sequence of RREQ and RREP messages. However, these techniques solely rely on reliability of the neighbouring node which is not always possible in the resource limited networks. A trusted model based authentication scheme was proposed by Liu *et al.* [20] to address the black-hole issue in WSNs. This model generates various routing paths with prior information about the attacker behaviours and compromised regions, which are susceptible to the malicious node(s), in WSNs. A node interested in transmission finds a trusted neighbour(s) via searching in its own trust database. This process not only secures the communication, but it improves the success ratio of packets. A chaotic feature based technique known as BP-AODV is presented by El-Semary and Diab [21] to resolve the black hole issue in mobile ad-hoc networks (MANETs). Although, this scheme is very effective against routing attacks, but the authentication is an energy consuming process. A forge packet based routing infrastructure, which is an enhanced version of the ad hoc on demand vector routing(AODV) scheme [22], [23], is presented to address the black-hole issue [24]. Fake route request RREQ messages, that is strongly correlated to the original messages, are transmitted to identify malicious nodes in WSNs. As these messages are known to the legitimate nodes, therefore, only malicious nodes will reply. A sensor node behaviours based routing infrastructure is presented by Shahabi *et al.* [25] to address the black-hole issue. Usually, a malicious node replies (rout reply RREP) to each and every route request (RREQ) messages received from neighbouring nodes. Moreover, the malicious node has the minimum possible hop count than legitimate nodes which is embedded in its RREP message(s). A malicious node has maximum RREP and minimum RREQ messages in the network whereas a legitimate node frequently initiates the rout request RREQ messages in the network. A neighbouring node activity based mechanism was presented to address the black-hole issue associated with point-to-point (P2P) devices networks [13]. For example, if a device, i.e., Node-A, sends a packet to another device, i.e., Node-B, then digital signature is used by Node-A to sign the packet which is verified by Node-B or other neighbouring devices via information maintained in their activity tables. Legitimate neighbouring nodes simply ignores this packet where a malicious or intruder node sends a PREPs message that is unsigned. Similarly, a timer based baited technique which consists of two phases was presented to resolve the black-hole issue [15]. A legitimate node uses a bait timer, i.e., 5 *u*sec, to generate and broadcast a message embedded with fake ID which is used to identify malicious nodes in its closed proximity. A trust value based routing mechanism is presented which bounds a node interested in communication to prefer a trusted path over the shortest path in an operational network [26]. The trust value of every intermediate node is computed, preferably after 0.07 *sec*, using their packets and PREQs forwarding abilities. This scheme is embedded in AODV based routing mechanism to prevent the black-hole attack. Likewise, an alternative approach where cross-checking of nodes, i.e., sender and neighbour to forward it further, is thoroughly performed to safeguard the network from black-hole attacks. To achieve this, every node has to maintain additional information in its routing table in the form of zero and one where 1 and 0 represent true and false values. Similarly, an AODV based scheme was presented by Hassan *et al.* [27] which is specifically designed for the smart meter networks. It uses two functions i.e., function-I updates sequence number at destination, if any RREQ is received whereas function-II denies DRREP acknowledgement from intruder node(s). Although, these techniques provides different ways to resolve the black-hole issue, however, these techniques are either applications specific or complex. Moreover, the probability of black-hole attack still exist and needed to addressed. A three-phase registration and authentication scheme were presented by He *et al.* [28] to address the device authenticity issue associated with resource limited networks. Although, this scheme was convincing as far as device authenticity is concerned, but it was overlay complex (due to three phases authenticity). Moreover, this scheme creates various overheads and compromises on lifetime of both individual devices and network. Similarly, a distributed query based authentication scheme was proposed by Ma *et al.* [29]. However, this scheme compromises on lifetime of individual nodes as these devices are bounded to use a complex encryption and decryption scheme.

III. PROPOSED METHODOLOGY: A HYBRID APPROACH

To resolve the aforementioned issue, i.e., black-hole attack specifically in the resource limited networks, a hybrid approach consists of medium access control (MAC) and AODV based protocol (MAC-AODV) is presented. Every device $C_i \in WSNs$ must have a valid MAC address that is shared with the concerned or nearest base station module S_j, particularly in offline phase, using appropriate cryptographic measures. The base station S_j decrypt this information and stores the device C_i in a repository or data dictionary i.e., MAC table. When a device, i.e., either a legitimate node C_i or an intruder node A_k, request to initiate the communication process with base station S_j then its authenticity is confirmed using MAC table information. Moreover, various encryption algorithms were incorporated in the proposed technique to achieve integrity and confidentiality of the collected data in the constraint oriented networks i.e., WSNs. The proposed hybrid scheme consists of two phase 1) Registration phase 2) Operational phase.

A. DEVICE REGISTRATION PHASE

In this phase which is off-line, every node or device C_i in WSNs generates a request message which includes its MAC address information and encrypts it using well-known encryption methods i.e., elliptic curve deffi-hellman problem (ECDDHP) and elliptic curve integrated encryption scheme (ECIES). In addition to the 48-bits MAC address, source and destination address information is included in the message generated by C_i. The encrypted message is sent to the concerned or nearest base station S_j which decrypt it using the aforementioned methods to collect the MAC address of sending device C_i. S_j adds the C_i's MAC address the data dictionary i.e., MAC table in this case. When MAC address is added to the MAC table then S_j sends a confirmation message to the concerned C_i in cypher text form. The concerned device or node C_i decrypt this message and updates it routing table entries. A detailed decryption of the off-line phase is presented in Figure. 2. Moreover, the registration (off-line phase) process is completed before the deployed network becomes operational i.e., starts it main function to achieve its target or goals. Therefore, the entrance probability of an intruder device A_k is almost negligible particularly in registration (off-line) phase. An intruder device A_k entry, specifically in off-line phase, is possible only if there is an adversary in the deployment team.

B. OPERATIONAL PHASE: LEGITIMATE DEVICE IDENTIFICATION

Every node $C_i \in WSNs$ is needed to be registered with the nearest base station S_j as described in subsection III-A preferably after the deployment phase through MAC addressing scheme where $i = 1, 2, 3, \ldots n$ and $j = 1, 2, 3 \ldots m$ such that $m < n$. It is to be noted that parameters m and n are adjusted according to the application requirements. Moreover, every S_j maintains a registration table, i.e., *MACTable*,

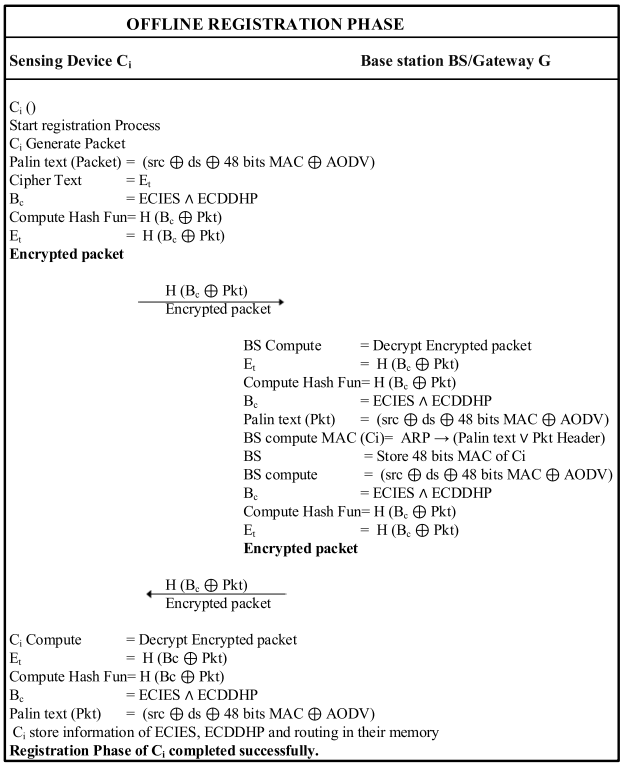

FIGURE 2. Offline phase: Devices registration process.

where member nodes information is stored, i.e., $C_i \in S_j$. A device/node C_i is allowed to trigger the communication process with a particular S_j **iff** C_i is registered with S_j i.e., $C_i \in member(S_j)$ or $C_i \in MACTable(S_j)$. For example, when a device $C_1 \in member(S_i)$ initiates the communication process with its concerned base station that is C_i sends an encrypted request message to the base station S_J. The concerned S_j module decrypts this message which contains requesting device information such as 48 bit MAC address, source and destination addresses. The concerned base station S_j ensures authenticity of the requesting device C_i through a cross-checking mechanism i.e., search the requesting device MAC address in its MAC table. If a match is encountered, that is $MAC(C_i) \in Registered(MAC)$, then requesting device C_i is allowed to start the communication activity that is transmission of its collected data. A complete description of this activity is depicted in Figure. 3.

C. OPERATIONAL PHASE: MALICIOUS DEVICE IDENTIFICATION

Conversely, if the requesting device A_k is a malicious or adversary node then,surely, it MAC address will not be registered with any base station S_j in an operational network and it is a mandatory step, particularly in the proposed mechanism, to initiate a communication process with any $S_j \in WSNs$. Hence, its request is denied by the concerned S_j as $MAC(A_k) \notin MACtable(S_j)$ where $k = 1, 2, 3 \ldots$.. Additionally, every neighbouring node resides in closed proximity,

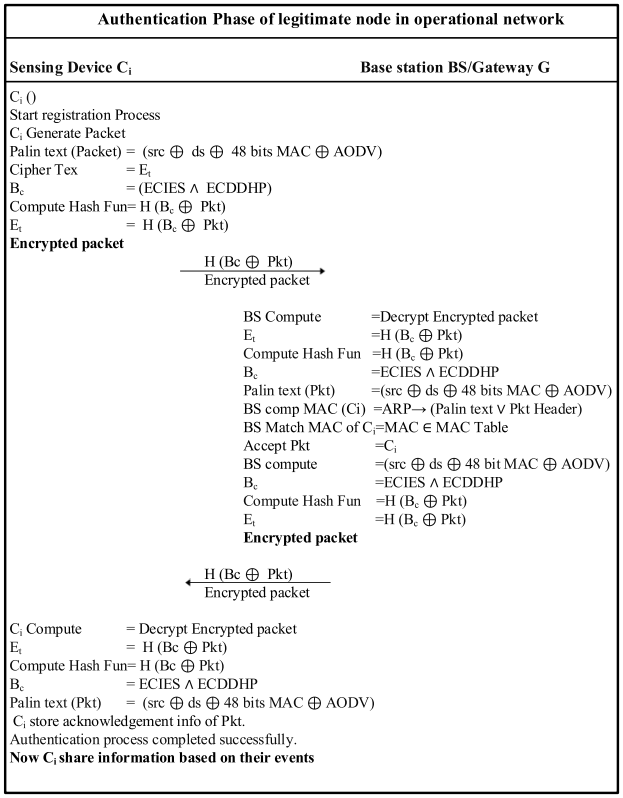

FIGURE 3. Operational phase: A legitimate node request initiation process with base station.

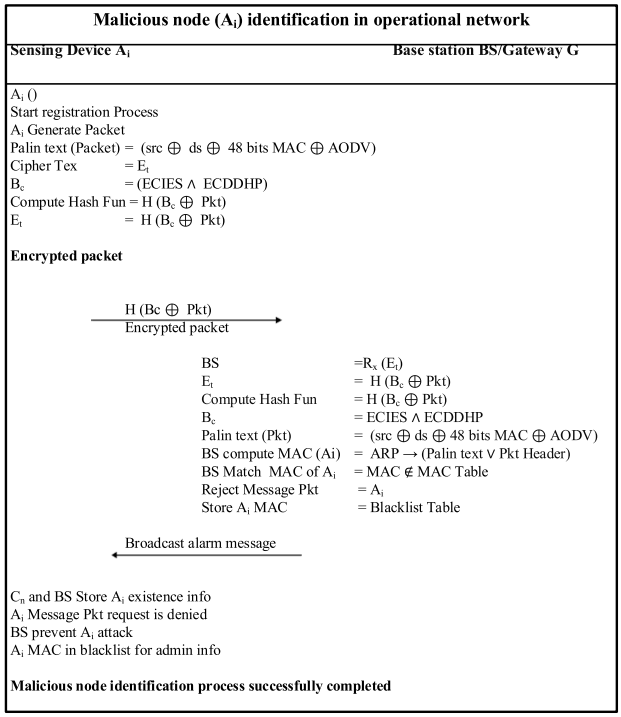

FIGURE 4. Operational phase: An intruder node request initiation process with base station.

i.e., $C_i \in S_j$, are informed about this malicious activity. The requesting process of A_k to initiate a communication session with a base station is depicted in Figure. 4.

The MAC based registration process of every C_i with its nearest S_j minimizes the probability of A_k in the operational WSNs. Moreover, the registration process of nodes C_i with a particular S_j is performed in an off-line phase as described above and S_j are prohibited to register further MAC addresses once the networks become operational. Hence, an intruder node A_k didn't find a way to mimic a legitimate node $C_i \in S_j$ and starts communication. Additionally, in the proposed scheme, every device C_i is assumed to have the ability to communicate directly with the concerned S_j in an operational network.

Moreover, every device C_i in an operational network has a defined waiting time, i.e., back-off time which is the time needed for a particular C_i to receive confirmation response from the concerned S_j module.

$$T_p = T_i(REQ) + T_r(RES) \tag{1}$$

where T_i represents the time needed for a request message generated a C_i to reach its destination i.e., S_j and T_r is the registration confirmation response time from S_j. T_p is used to differentiate the malicious nodes/devices A_k responses from legitimate one. Every legitimate device C_i waits for the confirmation response from S_j until T_p is expired which means either the request or the response is lost. Therefore, the process is repeated i.e., C_i resends the request packet to the concerned S_j for initiating a communication process.

Theorem-1: A device C_i generates an authentication or data processing request with the concerned S_j **iff** $C_i \in member(S_j)$.

Proof: Lets assume that, an intruder node A_k initiates an authentication request to the nearest sink S_j by sending its MAC address. S_j will authenticate the requesting device A_k by triggering a lookup operation where MAC of A_k is searched in registered MAC addresses table T_j. Since, a match is not available for the MAC of A_k, hence, S_j denies the request of A_k or simply ignore it. Conversely, if a legitimate node C_i initiates an authentication request to the concerned S_j then it will be verified successfully as MAC of $C_i \in member(S_j)$. Hence, only a legitimate node C_i, $C_i \in member(S_j)$ initiates a request to process the collected data.

Theorem-2: An authentication request is processed by a legitimate sink node S_j only.

Proof: Assume that an intruder node A_k intercepts an authentication request destined for a particular S_j. A_k needs to process this request within stipulated time i.e., waiting time of a legitimate device C_i represented by T_p to receive an authentication process confirmation from the intended S_i. Every device stores this information at the off-line phase where registration activity is performed. An intruder node A_k lacks this information and is unable to respond within stipulated time frame i.e., T_p. Additionally, in scenarios where a response from a particular S_j is intercepted by an intruder A_k

and forwards it with malicious information to the concerned C_i. A legitimate C_i has the capacity to differentiate this malicious packet from the original via its T_p i.e., C_i will observe an unusual delay. Hence, it will discard that packet.

Conversely, if $C_i's$ authentication request is processed by a legitimate S_j then C_i will receive the response within stipulated time i.e., T_p.

Hence, an authentication request is processed by a legitimate sink S_j only not an intruder device A_k.

Additionally, the proposed approach uses a 48-bits MAC addressing scheme where 24-bits represent the manufacturer ID and the remaining bits are used for the identification of an individual sensor node in an operational network. This scheme is quiet effective in differentiating legitimate nodes from the adversary node(s) specifically in the deployment phase i.e., C_i *or* $A_k \in (Legitimate-node-Class)$. Moreover, if an adversary node A_k attempts to initiate a data processing request which is denied by the intended base station S_j as described above in theorem-1 and the concerned BS adds the MAC address of this A_k node to its black list. Blacklist mechanism is adopted to avoid or prevent further disturbance or process initiation request generated by A_k as presented in Algorithm below. $Class-Authenticate$ is used to store MAC addresses of the legitimate nodes in an operational network whereas $Black - list$ class stored the blacklisted devices information which are represented by A_k in the proposed system. Variable i is used to represent the actual sensor nodes deployed in a particular infrastructure.

Algorithm 1 Proposed Light-Weight Authentication Algorithm for the Constraint Oriented Networks

Require: Authentication of the Requesting Devices C_i
Ensure: Authenticate or Black-list (C_i)

$Class - Authenticate \leftarrow$ Zero
$Black - list \leftarrow$ Zero
$i \leftarrow$ Total Nodes in WSNs
for every $C_i \in WSNs$ **do**
  Send MAC Address
  if MAC address ($C_i \in Class - Authen$) **then**
    C_i is allowed to initiate info processing req
  elseif MAC address ($C_i \notin Class - Authen$) **then**
    C_i is not allowed to initiate info processing req
    C_i is aided to class $Black - list_k$
  end if
end for
return Class-Authen and BlackList

The proposed scheme uses access control list (ACL) based gateways to prohibit unauthentic devices A_k from communication either with an S_j or C_i in an operation network specifically resource limited. ACL facilitates the administrator, S_j in this case, to control scalability of the underline network i.e., node dies or deployment and management of new nodes.

Well-known encryption schemes, i.e., elliptic curve deffi-hellman problem (ECDDHP) and elliptic curve integrated encryption scheme (ECIES), are adopted in the proposed algorithm to achieve the desired level of data authenticity and confidentiality specifically in the constraint oriented networks environments. These schemes are selected based on their connection with MAC addressing scheme and complexity.

IV. INFORMAL SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, the proposed scheme resilience against well-known security breaches or attacks is described in detail particularly in the operational WSNs. Some of these attacks and their prevention measures adopted by the proposed scheme is described below.

A. CLIENT IMPERSONATES ATTACKS

Suppose that an intruder node A_k tries to send a login information request, that is a request to trigger the communication process, to the concerned base station S_j in an operational WSN. A_k needs to use an encrypted version of its MAC address information, 48-bits in this case, and share it with S_j. The MAC address information of a client device C_i is not shared with its neighbouring nodes as we have assumed that every device C_i has the capacity to communicate directly with its concerned base station S_j. Moreover, breaking 48-bits MAC address will require 2^48 iterations to decipher a particular client device C_i message and it is beyond the processing capabilities of an ordinary node. Therefore, it is difficult for an intruder device A_k to mimic the behaviours of a legitimate node C_i in an operational network that is possible in existing schemes such as [18], [21]. Moreover, every C_i and S_j have a pre-defined turn around time T_r, the time in which a sender device expects a response from the concerned receiver. If a response message arrives after T_r is expired then it is considered as malicious response and is ignored.

B. SENSING DEVICE IMPERSONATION ATTACKS

Assume that an intruder A_k interrupts an ongoing communication process between a client device C_i and base station S_j by intercepting the transmitted messages. A_k tries to modify a captured message and re-transmit it to convince either a legitimate node C_i or a base station S_j that the message contents came from an authentic source. However, due to the limited computational capabilities of an ordinary node we believe that it is impossible to break a 48-bits encrypted message within stipulated time frame i.e., turn around time T_r as described above.Hence, in proposed communication and authentication infrastructure, the probability of device impersonation attack is negligible in operational networks that is possible in existing approaches such as [18], [21].

C. BASE STATION/GATEWAY IMPERSONATION ATTACK

The proposed scheme is prune against the base station/gateway S_j impersonation attack as every device C_i has a defined time frame in which its expects to receive a response from a concerned S_j. For example, an intruder node A_k tries to impersonate a base station S_j in the operational WSNs

TABLE 1. Security comparison of different schemes.

Security Property	[18]	[27]	[20]	[3]	[19]	[21]	Proposed Sch
Client Impersonate Attack	No	Yes	Yes	Yes	Yes	No	Yes
Sensing Device Impersonate Attack	No	Yes	Yes	Yes	Yes	No	Yes
Base Station Impersonate Attack	Yes	Yes	No	Yes	No	Yes	Yes
Eavesdropping Attack	No	No	No	Yes	Yes	Yes	Yes
Perfect Forward and Backward Secrecy	Yes	No	Yes	Yes	Yes	Yes	Yes
Man in the Middle Attack	No	No	No	Yes	Yes	Yes	Yes

by intercepting messages from various client devices C_i destined for that particular S_j. However, it is computationally expensive and beyond the processing capacities of sensor nodes to decipher the original message and re-broadcast an updated version within the defined time frame T_r. Moreover, the intruder device A_k needs to generate its own MAC table, which is generated in off-line phase in the proposed scheme. As opposed to the existing scheme [19], [20], this attack is not feasible in the proposed infrastructure specifically in operational mode.

D. EAVESDROPPING ATTACK

Suppose that an intruder node A_k collects each and every message which is transmitted in an operational WSN. These messages are re-transmitted in modified form on in-secure channel(s). However, eavesdropping is not feasible in the proposed authentication and communication infrastructure as every node C_i needs to transmit data in cipher form which is formed through well-known encryption methods as describe above. Moreover, both sensor C_i and base station S_j modules create their data dictionaries in off-line phase where deployment probability of an intruder device A_k is negligible.

E. PERFECT FORWARD AND BACKWARD SECRECY

Suppose that an intruder node A_k hijacks an ongoing transmission session between a legitimate node C_i and base station S_j. Although, the message are transmitted in cipher form, but if we assume that A_k has deciphered it and forwards an updated version of the original message. However, this processing is needed to be completed within a specified time frame, which is fixed in off-line phase. As we know that in the proposed infrastructure, both node C_i and base station S_j use message arrival time to differentiate an original message from a malicious one. Hence, the proposed scheme is prune to perfect forward and backward attack while existing scheme [27] are sensitive to this attack particularly in operation mode.

A comparative analysis of the proposed scheme security features against well-known and field proven schemes is presented in Table 1. In this table, an entry with Yes means that the scheme is prune or not-vulnerable to those attacks.

V. RESULTS AND PERFORMANCE EVALUATION

In this section, a detail description of the simulation results are presented to elaborate and verify the proposed scheme performance against field proven algorithms over different evaluation metrics such as throughput, packets delivery ratio, end to end delay and by launching various intruder attacks in an operational WSN etc. These algorithms were implemented in OMNET++, which is an open source simulation environment specifically designed for the constraint oriented networks (WSNs), using similar deployment and performance metrics. Initially, a random topological infrastructure with embedded propagation delay is adopted to mimic the real deployment process of the constraint oriented networks i.e., WSNs. Moreover, path loss ratio and interference parameters were kept constant for the whole network as these parameters are beyond the scope of our proposed authentication and communication infrastructure. Various parameters used in the simulation setup of the proposed infrastructure is presented in table 2. To comply with the real node deployment and lifetime issues, standard battery powers, available of different development platforms, are used such as libelium.

TABLE 2. WSN's simulation parameters.

Parameters	values
WSN Deployment Area	1000m * 1000m
Sensor Node	50, 100, 500, 1000
Base Station	One
Initial Energy (E_s)	52000 mAh
Residual Energy (E_r)	E_s-E_c
Packet Transmission Power Consumption (P_{T_x})	91.4 mW
Channel Delay (Ch_{delay})	10 milliseconds
Packet Receiving Power Consumption (P_{R_x})	59.1 mW
Idle Mode Power Consumption	1.27 mW
Sleep Mode Power Consumption	15.4 μW
Transceiver Energy (T_i)	1 mW
Transmission Range (T_r)	500m
Receiving Power Threshold (RTS_n)	1024 bits
Packet Size (P_{size})	128 bytes
Hop Count (H_c) of Base Station	0
Initial Hop Count (H_c) of Sensor Nodes	∞
Maximum Distance between Nodes	300m
Sampling Rate of sensor nodes	10 seconds
Topological Infrastructure	Static and Random
Malicious Nodes	5
Traffic Type	CBR and UDP
Attack Type	Black-Hole

The proposed scheme is compared with Ad hoc on demand distance vector (AODV) and enhance Ad hoc on demand distance vector (EAODV) based mechanism specifically from the black-hole attacks and routing perspective. The malicious node(s) A_k were deployed in operational networks of AODV-based, EAODV-based and proposed MAC-AODV based schemes preferably after the deployment phase. We have observed that a malicious node is easily adjusted, i.e., becomes a legitimate node, in an operational network (WSN in this case) particularly in AODV and EAODV-based

TABLE 3. Comparison table for computational cost.

Scheme	User/Client	Sensor Side	Server Side	Total Cost
Proposed scheme	$2T_h$	-	$2T_h + 6T_{RAN}$	$4T_h + 6T_{RAN}$
Abdelshafy et al. [18]	$5T_h + 5T_{XOR}$	$2T_h + 1T_{XOR}$	$2T_h + 6T_{XOR}$	$6t_h + 11T_{XOR}$
Hasan et al. [27]	$2T_h + 6T_{XOR}$	$2T_h + 5T_{XOR}$	$3T_h + 3T_{XOR}$	$7T_h + 14T_{XOR}$
Liu et al. [20]	-	$2T_h + 2T_{XOR}$	$1T_h + 2T_{XOR}$	$3T_h + 4T_{XOR}$
Gupta et al. [3]	$7T_h + 4T_{XOR}$	$4T_h + 4T_{XOR}$	$5T_h + 3T_{XOR}$	$16T_h + 11T_{XOR}$
Makhalouf et al. [19]	-	$2T_h + 6T_{XOR}$	$7T_h + 7T_{XOR}$	$9T_h + 13T_{XOR}$
El-Semary et al. [21]	-	$3T_h + 2T_{XOR}$	$9T_h + 6T_{XOR}$	$12T_h + 8T_{XOR}$

TABLE 4. Comparison of the communication cost.

Scheme	No. of Messages	No. of Bits
Proposed Scheme	6	6,144
Abdelshafy et al. [18]	5	24,546
Hasan et al. [27]	6	32,000
Liu et al. [20]	60	30,620
Gupta et al. [3]	5	3,038
Makhalouf et al. [19]	5	6,144
El-Semary et al. [21]	3	12,288

authentication schemes. However, the MAC address binding mechanism in the concerned base station S_j minimizes the adjustment probability of an intruder node A_k in an operational WSN.

A. COMPUTATIONAL COST

Due to the resource limited nature of WSNs, a security scheme with the lowest possible computational cost is preferred over a computationally expensive scheme(s) if it doesn't compromise on the security measures. Table 3 provides a detailed comparative analysis of the proposed scheme and field proven scheme in terms of the computational cost. In Table 3, T_h represents the time required to compute a hash function and T_{XOR} describes the exclusive OR operation. T_{ran} represents the random nonce used in communication infrastructure, however, as opposed to hash function(s) its computational cost is negligible. A blank entry is used to describe situations where a security scheme doesn't use that measure i.e., in Vaidya et al. sensor side authentication is not needed, hence, it is represented with "-". It is evident from the analysis in Table. 3 that the proposed scheme is more suitable for WSNs as it needs the lowest computational cost than its rival schemes.

B. COMMUNICATION COST

In order to compare the communication cost of the proposed with existing schemes, we have assumed only those messages which are necessary, including both off-line (if any) and on line phases, to establish a proper communication session between legitimate nodes in an operational network. It is evident from Table.4 that the proposed scheme has minimum communication overhead than existing approaches except [3], [19]. However, both of these mechanisms are computationally complex, i.e., needs more processing time, than the proposed scheme as shown in Table.3

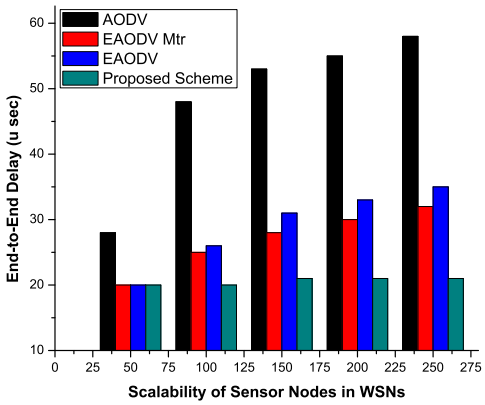

FIGURE 5. Comparative analysis of the proposed and existing schemes performance in term of end-to-end delay metric with various WSNs scalability.

C. END-TO-END DELAY

Generally in networking and particularly in WSNs, a communication or routing scheme with the lowest possible end-to-end delay ratio is considered as an ideal solution in different realistic environments. Therefore, performance of the proposed hybrid scheme in terms of end-to-end delay metric is compared with well-known techniques. Simulation results show that the proposed scheme performance is better than its rival schemes as shown in Figure. 5. Moreover, this parameter is highly effected, its value is decreased, if a technique is vulnerable to the black-hole attack(s). These results were obtained by introducing various malicious nodes in operational networks of the proposed and existing approaches.

D. AVERAGE THROUGHPUT

If the deployment process is random then the WSNs with relatively higher throughput, particularly with available resources, are preferred in various real scenarios or applications. In Figure.6, the throughput comparison of the proposed and existing schemes is presented which clearly depicts the exceptional performance of the proposed scheme.These measures were computed in the presence of various malicious nodes in the operational networks i.e., WSNs. As the proposed scheme is not susceptible to the black-hole attacks, conclusively, it results in better throughput than the rival schemes. Moreover, diverse scalability does not affect the proposed scheme performance specifically average throughput.

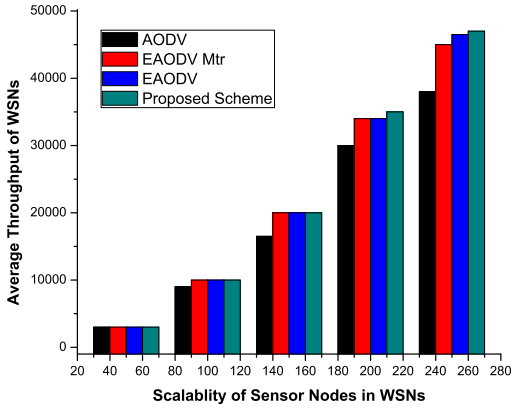

FIGURE 6. Comparative analysis of the proposed and existing schemes performance in terms of average throughput.

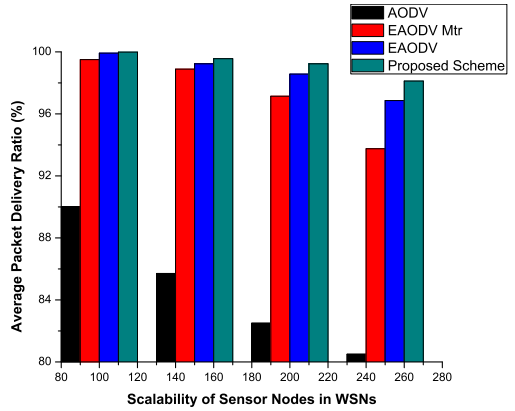

FIGURE 7. Comparative analysis of the proposed and existing schemes performance in terms of average packet delivery ratio.

E. AVERAGE PACKET DELIVERY RATIO

Packet delivery ratio describes the ratio of successfully received packets, particularly at the intended destination node(s), to the transmitted one and it is directly proportional to the average throughput of an operational network. The proposed scheme has a better performance ratio than the field proven schemes as shown in Figure. 7. Moreover, possibility of malicious node(s) activities, preferably black-hole attack, is thoroughly considered in the simulation environment and it is evident from Figure. 7 that the proposed scheme performance is not affected by these activities. It is due to the fact that the proposed scheme is not vulnerable to the black-hole attack.

VI. CONCLUSION AND FUTURE WORK

A tightly coupled issue with the resource limited networks, specifically WSNs, is the authentication process of various operational devices which becomes more complex if both sensor nodes & base station modules are mobile. Therefore, authentication scheme for these networks must be light-weight and should be smart enough i.e., accommodate easily in the changing topological infrastructures of WSNs. In this paper, a light-weight anonymous authentication techniques, MAC based AODV, for the constraint oriented networks was presented to resolve the aforementioned issue particularly black-hole attack. Every node was needed to be registered with its concerned (or nearest) base station that was carried out in an off-line phase. Intruder nodes were introduced in operational networks and it was observed that the proposed authentication scheme performance was incredible as malicious nodes' entry were almost impossible except, in scenarios, if melodious nodes were deployed at the off-line phase. Moreover, a hybrid data encryption scheme, elliptic curve integrated encryption standard (ECIES) and elliptic curve Deffi-Hellman problem (ECDDHP), was used to further strengthen the authenticity, confidentiality and integrity of both data and nodes. Simulation results verified the proposed scheme exceptional performance against its rival techniques particularly in achieving minimum end-to-end delay & communication cost, maximum average packet delivery ratio and throughput.

In the future, we are eager to extend the proposed authentication scheme to make it applicable for the multi hop communication infrastructure as well. Moreover, device-to-device or node-to-node authentication is needed to incorporated in the proposed scheme as direct communication of sensor node(s) with base station is not always possible and realistic.

ACKNOWLEDGMENT

The authors acknowledge Department of Computer Science Abdul Wali Khan University Mardan, Pakistan, for providing lab facilities.

REFERENCES

[1] A.-C. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "SD-WISE: A software-defined WIreless SEnsor network," *Comput. Netw.*, vol. 159, pp. 84–95, Aug. 2019.
[2] C. Savaglio, P. Pace, G. Aloi, A. Liotta, and G. Fortino, "Lightweight reinforcement learning for energy efficient communications in wireless sensor networks," *IEEE Access*, vol. 7, pp. 29355–29364, 2019.
[3] A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Comput. Netw.*, vol. 149, pp. 29–42, Feb. 2019.
[4] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.
[5] I. Tomic and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017.
[6] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, Jan. 2016.
[7] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.
[8] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.
[9] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, 2017.
[10] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the Internet of Things," *Comput. Netw.*, vol. 102, pp. 83–95, Jun. 2016.

[11] Y.-J. Liu, M.-Z. Sun, L. Zhou, and L. Lu, "Analysis on the principles of congestion charging policy and study on the decision-making model," *Procedia Eng.*, vol. 137, pp. 836–842, Jan. 2016.
[12] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Trans. Services Comput.*, to be published.
[13] P. Ndajah, A. O. Matine, and M. N. Hounkonnou, "Black hole attack prevention in wireless Peer-to-Peer networks: A new strategy," *Int. J. Wireless Inf. Netw.*, vol. 26, no. 1, pp. 48–60, Dec. 2018.
[14] Q. M. Yaseen and M. Aldwairi, "An enhanced AODV protocol for avoiding black holes in MANET," *Procedia Comput. Sci.*, vol. 134, pp. 371–376, Jan. 2018.
[15] A. Yasin and M. Abu Zant, "Detecting and isolating black-hole attacks in MANET using timer based baited technique," *Wireless Commun. Mobile Comput.*, vol. 2018, Sep. 2018, Art. no. 9812135.
[16] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *Proc. IEEE 6th Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Oct. 2010, pp. 600–606.
[17] H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Global Telecommun. Conf.*, Nov. 2007, pp. 986–990.
[18] M. A. Abdelshafy and P. J. King, "AODV and SAODV under attack: Performance comparison," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*. Benidorm, Spain: Springer, 2014, pp. 318–331.
[19] A. Meddeb Makhlouf and M. Guizani, "SE-AOMDV: Secure and efficient AOMDV routing protocol for vehicular communications," *Int. J. Inf. Secur.*, vol. 18, no. 5, pp. 665–676, Apr. 2019.
[20] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.
[21] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map," *IEEE Access*, vol. 7, pp. 95197–95211, 2019.
[22] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 6, no. 3, pp. 106–107, 2002.
[23] B. Karthikeyan, S. Hari Ganesh, and N. Kanimozhi, "Security improved ad-hoc on demand distance vector routing protocol (SIm AODV)," *Int. J. Inf. Sci. Comput.*, vol. 10, no. 2, pp. 32–37, 2016.
[24] T. Delkesh and M. A. Jabraeil Jamali, "EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs," *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 5, pp. 1897–1914, Mar. 2018.
[25] S. Shahabi, M. Ghazvini, and M. Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack," *Wireless Netw.*, vol. 22, no. 5, pp. 1505–1511, Aug. 2015.
[26] R. K. Bar, J. K. Mandal, and M. M. Singh, "QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack," *Procedia Technol.*, vol. 10, pp. 530–537, Dec. 2013.
[27] M. R. Hasan, Y. Zhao, Y. Luo, G. Wang, and R. M. Winter, "An effective AODV-based flooding detection and prevention for smart meter network," *Procedia Comput. Sci.*, vol. 129, pp. 454–460, Jan. 2018.
[28] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," in *Proc. Int. Symp. Wireless Pervas. Comput. (ISWPC)*, Nov. 2013, pp. 1–6.
[29] C. Ma, K. Xue, and P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks," *Secur. Commun. Netw.*, vol. 7, no. 4, pp. 759–773, Apr. 2013.

MUHAMMAD ADIL received the B.S. (CS) degree in computer science from the Virtual University of Pakistan, Lahore, in 2016, where he is currently pursuing the M.Sc. (CS) degree in computer networks from the Department of Computer Science. His research interests include different routing protocols, security in WSN, the IoT, and machine learning techniques.

RAHIM KHAN received the Ph.D. degree in computer system engineering from the Ghulam Ishaq Khan Institute (GIKI), Swabi, Pakistan. He is currently an Assistant Professor with the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. His research interests include wireless sensor networks (WSNs) deployment, the Internet of Things (IoT), routing protocols, outliers detection, techniques for congestion control, decision support system (DSS), vehicular ad hoc networks, data analysis, and similarity measures.

MOHAMMED AMIN ALMAIAH received the M.Sc. degree in computer information system from Middle East University (MEU), Jordan, in 2011, and the Ph.D. degree in computer science from Universiti Malaysia Terengganu, Malaysia. He is currently working as an Assistant Professor at the Department of CIS, King Faisal University, Saudi Arabia. He has published over 15 research papers in highly reputed journals, such as the *Engineering and Science Technology, an International Journal*, *Education and Information Technologies*, and *Journal of Educational Computing Research*. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include mobile learning, software quality, network security, and technology acceptance. He is a certified recognized Reviewer in IEEE, Elsevier, and Springer.

MOHAMMED AL-ZAHRANI is currently a Faculty Member with the College of Computer Science and Information Technology, King Faisal University, Saudi Arabia, where he is also the Dean of the Information Technology Unit. He has several international publications to his credit and has vast consultancy experience in networks. His research interests include wireless sensor networks and the Internet of Things.

MUHAMMAD ZAKARYA received the Ph.D. degree in computer science from the University of Surrey, Guildford, U.K. He is currently a Lecturer with the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. His research interests include cloud computing, mobile edge clouds, performance, energy efficiency, algorithms, and resource management. He has deep understanding on the theoretical computer science and data analysis. Furthermore, he also owns deep understanding on various statistical techniques which are, largely, used in applied research.

MUHAMMAD SAEED AMJAD received the M.S. degree in computer science from NCBA & E, Lahore, and the master's degree in information technology from the University of the Punjab, Pakistan. After completing his master's degree, he joined the Army Public College of Management Sciences (APCOMS), Gujranwala, as a Computer Lecturer and has been teaching various subjects related to computer science and information technology for one and half year. He also has to his credit the experience of serving Pakistan Army Aviation for one and half year as a Network Supervisor. He has been a member of the Faculty of Computer Science and Information Technology, Virtual University of Pakistan, since November 2010. His major area of interest is computer networks.

REHAN AHMED received the B.E. degree in computer systems from the Quaid-e-Awam University of Engineering Sciences and Technology, Nawabshah, Pakistan, and the M.Phil. degree in computer science. He has been serving as an Instructor with the Department of Computer Science, Virtual University of Pakistan, since September 2007. His main area of interest is computer networks. He has to his credit the experience of teaching at the Nawab Shah Institute of Information Technology, for one year, as a Computer Lecturer. He also has the experience in Policy Planning Cell, Ministry of (L&M) Islamabad, for one and half year, as a Data manager.