DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5893

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AN INVESTIGATION STUDY ON ENERGY EFFICIENT AUTHENTICATION TECHNIQUES IN WIRELESS SENSOR NETWORK

Antony Cynthia
Ph.D. Research Scholar,
Department of Computer Science,
Hindusthan College of Arts and Science, Coimbatore,
Tamil Nadu, India

DR. V. Saravanan,
Head and Associate professor,
Department of Information Technology,
Hindusthan College of Arts and Science, Coimbatore,
Tamil Nadu, India

Abstract: Wireless sensor networks (WSNs) are ubiquitous technology for the growth of low cost and low power wireless technology. WSN is the collection of spatially distributed sensors for sensing the physical conditions and organizing the collected data. Sensor nodes have lesser transmission range with limited storage capabilities and energy resources. Routing protocols in WSN guarantee the reliable multi-hop communication from the source node to destination node. An Authentication process is carried out to identify the authorized user for secured routing. In existing authentication methods, key management schemes and hashing techniques were used for increasing the authentication and security level performance. However, the existing techniques failed to improve the authentication accuracy and reduce the authentication time with minimal energy consumption (EC) for secured data transmission in WSN. This paper studied the problem faced using existing authentication techniques in order to increase the security level.

Keywords: Wireless sensor networks, Routing, Sensor nodes, authentication, multi-hop communication**,** key management**.**

I. INTRODUCTION

WSN comprises the number of small sensor nodes for broadcasting the information over wireless links. Nodes comprise the sensing and broadcasting abilities. Sensor nodes are battery controlled in terms of energy, and storage in many applications like examination, observation, and monitoring. In WSN, sensor nodes are used to execute the sensing tasks within the operation area. With minimal energy resources, nodes collect the information from the physical environment, process data and send the information. EC is a key challenge in WSNs as it impacts network lifetime (NL) in absence of human involvement. The nodes depend on short-range communication and form the multi-hop network for information delivery to the base station. Routing in WSN is the process of transmitting the data from the source to data sink in the energy-efficient method. Security is an essential problem in WSN while routing the information from the source node to destination node.

The paper is structured as follows: Section 2 explains the review on different energy efficient authentication techniques in WSN, Section 3 describes the study and analysis of the existing authentication techniques, Section 4 portrays the possible comparison of existing techniques. In Section 5, limitations of the existing authentication techniques are studied with future direction and Section 6 concludes the paper.

II. LITERATURE SURVEY

An active detection secured routing scheme termed Active Trust (AT) was designed in [1] for WSNs. AT eradicates black holes for detect and achieves nodal trust for improving data route security. By resolving NLP, equivalent energy allocation with routing probabilities is accomplished. But, the authentication accuracy was not improved. A state space battery model was introduced in [2] with optimal policy comprised the time-invariant routing probabilities in fixed topology network and addressed the set of Non-Linear Programming (NLP) issues. But, the probabilistic nature of routing policies was not developed for addressing the security threats when operating under many attack conditions.

A provably secure pairing-free ID-based signature scheme was presented in [3] with message recovery. However, communication cost was high. In [4], an effective key management protocol (CL-EKM) was introduced for secured routing. It is exploited for key updates while node leaves or joins a cluster. However, CL-EKM protocol failed to identify the public key verifiability property for reducing the unnecessary burden on decryptor while decrypting invalid keys. A new Linear Programming Framework was designed in [5] depending on the route energy cost for increasing the security level in WSN. But, LP framework was not used for different features of route diversity with lesser energy dissipation.

The challenges for network coverage, NL, and physical design were addressed in [6] to handle the harsh environments. An enhanced and efficient cluster-based security protocol was introduced in [7] for end-to-end data authentication with the digital signature and increased the efficiency through security analysis. But, en-route filtering mechanism failed to protect the intermediate nodes from forgery due to the absence of authentication codes. A new authentication scheme was presented in [8] for WSN. The random oracle model revealed formal proof and employed the protocol for the formal verification process. But, the mutual authentication between nodes was not carried out to increase the security level.

III. ENERGY EFFICIENT AUTHENTICATION TECHNIQUES IN WIRELESS SENSOR NETWORK

WSN has any number of sensor nodes for sensing the tasks within operation area. With inadequate energy resources, the nodes sense the physical phenomena like temperature, vibrations, sounds, etc., and transmit the information to sink node. The nodes cooperate with each other to complete the assigned tasks. Data are transmitted in a network by forwarding the data from one node to another node in multiple-hop transmission. Routing is the process of transmitting the data from the source node to destination node. Secured routing of the sensed data is a key demand in WSN. Authentication is one of the security goals for the data communication in WSN. Authentication assures the receiver that data originates from the correct source node. The existing authentication techniques are discussed in following sub-section.

A. ActiveTrust: Secure and Trustable Routing in Wireless Sensor Network

An active security and trust routing scheme termed AT is introduced for WSN. Active Trust avoids the black holes for route identification and for trust enhancement. To attain security in WSN, AT provides construction and distribution of detected routes to make detection routes. AT is a routing scheme employed for Black Hole Attack (BLA) identification with active detection routing. In AT, Several routes are identified with residual energy. The Attacker is not vulnerable to detection routes.

In WSN, energy is expensive. When active detection is processed, EC is high. It is not feasible to imagine greater energy nodes for active detection routes. For route detection, AT includes high residue energy and lessens the EC. Detected routes identify the nodal trust without minimizing NL and enhancing security. With the shortest and multipath routing, the energy efficiency of AT scheme is increased more than 2 times. It improves the security results. In AT, nodal trust was obtained. The nodes with high trust are selected to eliminate the attack.

The data routing is the process of collecting the data packet and choosing one node near sink whose trust is higher than the threshold as next hop. When node failed to identify any appropriate next hop node, it sends the feedback malfunction to the upper node. The upper node recomputed the unselected node set. It chooses the node with the largest trust similar to the next hop. When it failed to identify the next hop, it transmits the feedback failure to the upper node.

B. BASIS: A Practical Multi-User Broadcast Authentication Scheme for Wireless Sensor Networks

WSN includes sink node, sensor node, and users. WSN provides the information services to many network users that travel in the network to sink. The sink provides Private Key Generator (PKG) for generating the private keys of users. PKG is managed with sufficient computation and storage ability. Message broadcasters are sink and users that are linked with devices than sensor nodes in terms of computation ability and energy. The sink sends the administrative command and network users send the queries/commands through sensor nodes in the vicinity and expect replies with latest network information. The users join in WSN dynamically and repealed due to the membership variations or compromise. Sensor nodes are resource limited regarding the memory space, computation ability and bandwidth.

Adversaries in WSNs are divided into two types, namely external or internal adversaries. The external adversaries failed to include the authentic keying material to connect to the network functions as legitimate nodes. Internal adversaries with authentic keying material of legitimate nodes are difficult one to protect against the external ones. The adversaries eavesdrop on radio transmissions or insert the bogus data or routing messages into the network to utilize a large number of network resources. It communicates and collaborates with high bandwidth and low-latency channel to valid sensor nodes. The low-cost sensors are used in unattended target field that is insecure against the node capture attacks.

Multi-user broadcast authentication is a security model for mobile users of WSN broadcasts messages dynamically and reliably. In order to minimize the communication costs due to transmission, authentication techniques are introduced for identity-based cryptography. The designed scheme experiences the expensive pairing computations. Applying [3] the computation and communication costs were reduced. For authentication among user and sink, An ID-based multi-user broadcast authentication technique is presented.

An IBS scheme with message recovery is known as MR-IBS and IBS scheme with partial message recovery are termed as PMR-IBS. The designed scheme is secure in random oracle model for addressing Elliptic Curve Discrete Logarithm issue. A practical ID-based multi-user BA scheme called BASIS was introduced depending on MR-IBS and PMR-IBS for broadcast authentication of users and sink to reduce the communication costs. The security of BASIS for authenticity is minimized in the formal security model. The feasibility of BASIS on WSN hardware platforms such as MICAz and Tmote Sky are evaluated using computation/communication cost and EC.

C. Energy-based Lifetime Maximization and Security of Wireless Sensor Networks with General Non-ideal Battery Models

A state space battery model was introduced with optimal policy comprised the time-invariant routing probabilities in fixed topology network. With the higher NL, A joint routing and energy distribution issues are addressed. Sensor NL improved by routing and energy allocation on nodes. In dynamic battery model, optimal policies include time-invariant routing probabilities in network topology and solve the NLP issues.

The issues are reformulated as single NLP. The solution to a problem is afforded through lessening every node energy at the same time. Through addressing NLP problem, energy allocation and routing probabilities are attained. Network performance enhances NL and throughput under security problems and faked-cost attacks.

The joint routing and initial energy allocation issues are addressed for NL maximization through implementing non-ideal battery model. The time-invariant nature of NL routing policy is protected. The optimal policies are certainly robust regarding the battery model. The corresponding NL value is different. The designed model is used to minimize

computational complexity for optimal routing policy. An efficient single NLP formulation is carried out for addressing NLP problems.

WSN performance is improved by solving the security risks. Energy-aware routing policies are probabilistic and it is hard for attackers to recognize ideal node. The probabilistic routing policy is employed as the deterministic policy through changing the probabilities to packet flows. The network performance is not improved due to the existence of routing attacks in WSN.

D. Effective Key Management in Dynamic Wireless Sensor Networks

CL-EKM is introduced for secured routing in WSN. The designed protocol maintains key revocation for compromised nodes and reduces the impact of node compromise on the security of additional communication links. In certificate-less public key cryptography (CLPKC), the user full private key is a mixture of the partial private key created by key generation center (KGC) and user secret value. The organization of full private/public key pair eliminates the requirement for certificates and addresses key escrow issue through eliminating the responsibility for user full private key.

The merits of ECC keys are described on an additive group with 160-bit length. For node authentication and pair-wise key identification, CL-EKM is constructed with pairing-free certificate less hybrid sign encryption scheme (CL-HSC). With CL-HSC, the pair-wise key of CLEKM is distributed between two nodes without pairing and certificate exchange. CL-EKM supports the lightweight processes for cluster key updates when a node moves. Key revocation is carried out when the node is identified as malicious or lefts the cluster. CLEKM is scalable during new node addition after network exploitation.

IV. COMPARISON OF ENERGY EFFICIENT AUTHENTICATION TECHNIQUES IN WIRELESS SENSOR NETWORK

In order to compare the energy efficient secured routing using different techniques, the number of sensor nodes and packets is taken to perform the experiment. For performing the energy efficient secured routing experiment, parameters such as authentication time, energy consumption, authentication accuracy and security level are used.

A. Authentication Time

Authentication time is defined as the amount of time taken to perform the authentication process for improving the security level. Authentication time is the difference between starting time and ending time of authentication process. It is measured in terms of milliseconds (ms). It is mathematically formulated as,

Authentication time=starting time-ending time (1)

Lesser the authentication time, more efficient method is said to be.

Table I. Tabulation for Authentication Time

Number of Sensor Nodes (Number)	Authentication Time (ms)			
	Active Trust	Provably secure pairing-free ID-based signature scheme	State space battery model	CL-EKM Protocol
10	65	72	77	83
20	68	74	82	87
30	71	77	85	90
40	73	80	87	93
50	75	83	91	96
60	78	85	94	99
70	81	89	97	103
80	85	92	101	106
90	89	95	104	109
100	94	98	107	112

Table 1 explains authentication time with respect to the number of sensor nodes ranging from 10 to 100. Authentication time comparison takes place on existing Active Trust, Provably secure pairing-free Identity-based signature scheme, State space battery model, and CL-EKM protocol. From the table value, it is observed that the authentication time using AT is lesser when compared to provably secure pairing-free ID-based signature scheme, State space battery model and CL-EKM Protocol.

The graphical representation of authentication time is described in figure 1.

Figure 1Measure of Authentication Time

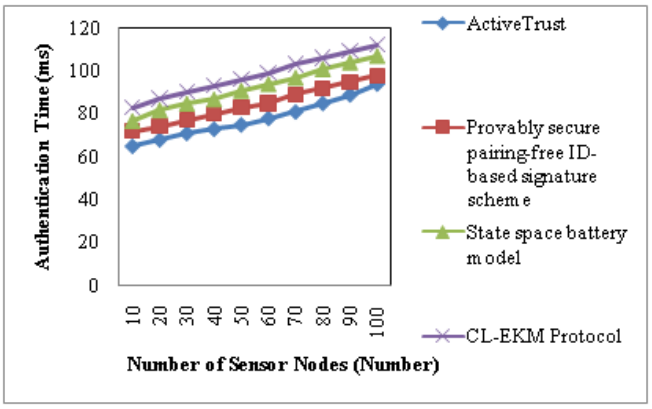

Figure 1 explains the authentication time comparison for four different existing methods, namely AT, Provably secure pairing-free Identity-based signature scheme, State space battery model, and CL-EKM protocol. From the above graph, it is observed that authentication time of AT is lesser than State space battery model, provably secure pairing-free Identity-based signature scheme and CL-EKM protocol.

Different routes are discovered in AT region with residue energy. The attacker is not susceptible to detection routes. BLA is eradicated by attacker behavior and nodal trust through detecting the data routes. This helps to minimize the authentication time. The authentication time of AT is 8% lesser than provably secure pairing-free Identity-based signature

scheme, 16% lesser than State space battery model and 20% lesser than CL-EKM protocol.

B. Authentication Accuracy (AA)

Authentication accuracy is defined as the ratio of the number of correctly authenticated sensor nodes to the total number of sensor nodes. It is measured in terms of percentage (%). It is mathematically formulated as,

$$AA=\frac{\text{number of correctly authenticated sensor nodes}}{\text{Total number of sensor nodes}} \quad (2)$$

Higher the authentication accuracy, more efficient method is said to be.

Table II Tabulation for Authentication Accuracy

Number of Sensor Nodes (Number)	Authentication Accuracy (%)			
	Active Trust	Provably secure pairing-free ID	State space	CL-EKM Protocol
10	65	81	68	71
20	67	82	70	73
30	68	84	72	75
40	70	86	73	76
50	71	87	74	78
60	72	89	76	80
70	74	91	77	81
80	76	93	79	82
90	79	94	81	85
100	81	96	84	87

Table 2 explains authentication accuracy with respect to the number of sensor nodes ranging from 10 to 100. Authentication accuracy comparison takes place on existing AT, Provably secure pairing-free Identity-based signature scheme, State space battery model, and CL-EKM protocol. From table value, it is observed that the authentication accuracy using provably secure pairing-free ID-based signature scheme is higher when compared to Active Trust, State space battery model, and CL-EKM Protocol. The graphical representation of authentication accuracy is shown in figure 2.

Figure2:MeasureofAuthenticationAccuracy

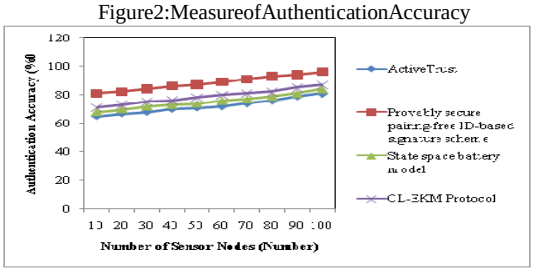

Figure 2 describes the authentication accuracy comparison for four different existing methods, namely AT, Provably secure pairing-free Identity-based signature scheme, State space battery model, and CL-EKM protocol. From above-mentioned graph, it is clear that authentication accuracy of provably secure pairing-free Identity-based signature scheme is lesser than AT, State space battery model, and CL-EKM protocol. In the provably secure pairing-free Identity-based signature scheme, energy-aware routing policies are probabilistic and it is difficult for attackers to identify the ideal node. The probabilistic routing policy used deterministic policy by varying the probabilities of packet flows. This helps to increase the authentication accuracy. The EC of state space battery model is 22% higher than AT, 17% higher than Provably secure pairing-free Identity-based signature scheme and 12% higher than CL-EKM protocol.

C. Energy Consumption (EC)

EC is defined as the product of the number of sensor nodes and amount of energy consumed by one sensor node. It is measured in terms of joules (J). It is mathematically formulated as,

$$EC=n*\text{energy consumed by one sensor node} \quad (3)$$

Lesser the energy consumption, more efficient method is said to be.

Table III Tabulation for Energy Consumption

Number of Sensor Nodes (Number)	Energy Consumption (J)			
	Active Trust	Provably secure pairing-free ID-based signature scheme	State space battery model	CL-EKM Protocol
10	78	69	65	81
20	82	71	68	84
30	85	75	72	88
40	88	78	75	92
50	91	82	78	96
60	95	85	81	98
70	99	89	84	104
80	105	91	87	109
90	108	93	91	115
100	112	97	94	121

Table 3 illustrates the EC with respect to the number of sensor nodes ranging from 10 to 100. EC comparison takes place on existing AT, Provably secure pairing-free Identity-based signature scheme, State space battery model, and CL-EKM protocol. From table value, it is clear that the EC using State space battery model is lesser when compared to AT, provably secure pairing-free ID-based signature scheme and CL-EKM Protocol. The graphical representation of EC is shown in figure 3.

Figure 3 Measure of Energy Consumption

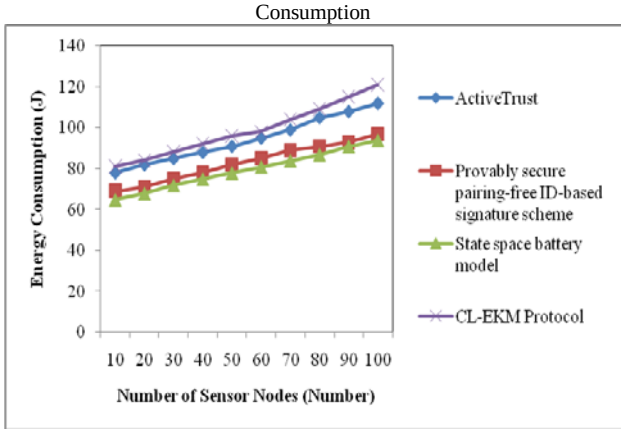

Figure 3 portrays the EC comparison for four different existing methods, namely Active Trust, Provably secure pairing-free Identity-based signature scheme, State space battery model, and certificate-less effective key management (CL-EKM) protocol.

From above graph, it is clear that EC of State space battery model is lesser than Active Trust; provably secure pairing-free Identity-based signature scheme and certificate-less effective key management (CL-EKM) protocol. In state space battery model, energy-aware routing policies are probabilistic and it is difficult for attackers to identify the ideal node.

The probabilistic routing policy used deterministic policy by varying the probabilities to packet flows. This helps to reduce the energy consumption. The EC of state space battery model is 16% lesser than AT, 4% lesser than provably secure pairing-free Identity-based signature scheme and 19% lesser than certificate-less effective key management (CL-EKM) protocol.

D. Security Level

Security level (S) is defined as the ratio of data packets sent and packets received during the routing process. It is measured in terms of percentage (%). It is formulated as,

$$S = \frac{Data\ Packets_r}{Data\ Packets_s} * 100 \qquad (4)$$

From (4) security's' is calculated based on packets and packets received packets. Higher the security level, more efficient the technique is to be.

Table 4 Tabulation for Security Level

Number of Data Packets Sent (Number)	Security Level (%)			
	Active Trust	Provably secure pairing-free ID-based signature scheme	State space battery model	CL-EKM Protocol
50	65	69	74	81
100	66	71	76	83
150	68	73	77	84
200	70	75	79	86
250	71	76	81	87
300	73	78	83	89
350	74	79	84	91
400	75	81	86	92
450	77	82	88	93
500	79	84	90	95

Table 4 describes the security level with respect to the number of packets ranging from 50 to 500. Security level comparison takes place on existing AT, Provably secure pairing-free Identity-based signature scheme, State space battery model and certificate-less effective key management (CL-EKM) protocol.

From the table, it is observed that the security level using certificate-less effective key management (CL-EKM) protocol is higher when compared to AT, provably secure pairing-free ID-based signature scheme and State space battery model. The graphical representation of security level is illustrated in figure 4.

Figure 4 Measure of Security Level

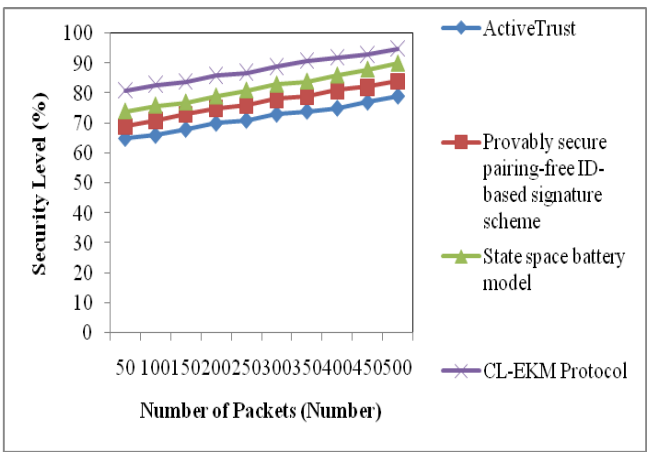

Figure 4 explains the security level comparison for four different existing methods, namely AT, Provably secure pairing-free Identity-based signature scheme, State space battery model, and CL-EKM protocol. From the above-mentioned graph, it is clear that security level of CL-EKM protocol is higher than AT, Provably secure pairing-free Identity-based signature scheme and state space battery model. CL-EKM protocol protects the key revocation for cooperated nodes and reduces the node compromise on security. This helps to increase the security level. The security level of CL-EKM protocol is 23% higher than AT, 15% higher than provably secure pairing-free Identity-based signature scheme and 8% higher than state space battery model.

V. DISCUSSION AND LIMITATION ON ENERGY EFFICIENT AUTHENTICATION TECHNIQUES IN WSN

In AT scheme, generation and distribution of identified routes were given. To improve security and energy efficiency performance, AT scheme utilizes energy in non-hotspots. AT increases route success rate and detected against BLA with higher NL. AT eliminated the black holes by finding the multiple detection routes for increasing the data route security. But, the authentication accuracy was not improved out due to the presence of black-hole attacks.

State space battery model was introduced for solving the NLP problems. By solving NLP problem, the energy allocation and routing possibilities are attained. A joint routing and energy allocation issues addressed over network nodes with improved NL. Probabilistic routing policies do not employ for addressing the security threats with higher performance level while operating at multiple attack conditions.

In [3], a message recovery with minimized computation and communication cost was presented. The feasibility of BASIS on WSN was introduced to minimize the energy consumption. CL-EKM was introduced for secured routing in WSN through node mobility. CL-EKM protocol failed to identify the public key verifiability property for reducing the unnecessary burden on decryptor while decrypting the invalid keys. The mathematical model for EC was not reduced in CL-EKM regarding node movements.

A. Related Works

The inefficient use of watchdog technique leads to the planning of new optimization method in [9] for minimizing the energy cost of watchdog and for increasing the security. But, watchdog tasks identified the preliminary solutions for monitoring the energy consuming units. A secure and efficient mutual-healing protocol was designed in [10] with Chinese Remainder Theorem (CRT) based secret sharing for key broadcast. Though mutual-healing protocol was used for group key broadcast, the security was not enhanced and accessed by an unauthorized member.

A mutual authentication protocol was presented in [11] with the timestamp in WSN. The designed protocol generated a new session key for every session. Elliptic Curve Diffie–Hellman in mutual authentication protocol presented maximum cryptographic strength per bit. But, ECDH was difficult to improve security for standard curves. A fountain-coding aided relaying scheme was designed in [12] where all source packets were encoded with fountain codes are sent over channels. A cooperative jamming method was employed to reduce the received signal quality at eavesdropper. But, the robustness of fountain-coding aided relaying scheme was not improved due to the imperfect channel state information transmitter (CSIT) at jammer.

VI. FUTURE DIRECTION

The future direction of energy-efficient authentication techniques in WSN can be carried out using cryptographic techniques for improving the authentication accuracy and security level during routing.

VII. CONCLUSION

A comparison of different existing energy efficient authentication techniques during routing in WSN is studied. From the study, it is observed that the existing techniques failed to improve the performance of authentication accuracy and energy consumption. The survival review shows that the existing CL-EKM protocol failed to identify the public key verifiability. In addition, security threat problems are not addressed. The wide range of experiments on existing techniques studies performance of many energy efficient authentication techniques with its limitations. Finally, from the result, the research work can be carried out using cryptographic techniques for improving the performance of security during routing the information in WSN.

VIII. REFERENCES

[1] Yuxin Liu, Mianxiong Dong, Kaoru Ota, and Anfeng Liu, "ActiveTrust:Securely and Trustable Routing inWireless Sensor Networks", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 9, September 2016, Pages 2013 – 2027

[2] Sepideh Pourazarm and Christos G. Cassandras, "Energy-based Lifetime Maximization and Security of Wireless Sensor Networks with General Non-ideal Battery Models", IEEE Transactions on Control of Network Systems, Volume 4, Issue 2, June 2017, Pages 323 – 335

[3] Kyung-Ah Shim, "BASIS: A Practical Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, Volume 12, Issue 7, July 2017, Pages 1545 – 1554

[4] Seung-Hyun Seo, Jongho Won, Salmin Sultana, and Elisa Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, Volume 10, Issue 2, February 2015, Pages 371 - 383

[5] Davut Incebacak, Kemal Bicakci and Bulent Tavli, "Evaluating Energy Cost of Route Diversity for Security in Wireless Sensor Networks", Computer Standards & Interfaces, Elsevier, Volume 39, March 2015, Pages 44-57

[6] Jakob Pilegaard Juul, Ole Green and Rune Hylsberg Jacobsen, "Deployment of Wireless Sensor Networks in Crop Storages", Wireless Personal Communications, Springer, Volume 81, Issue 4, April 2015, Pages 1437–1454

[7] Huei-Wen Ferng and Nguyen Minh Khoa, "On security of wireless sensor networks: a data authentication protocol using digital signature", Wireless Networks, Springer, Volume 23, Issue 4, May 2017, Pages 1113–1131

[8] Fan Wu, Lili Xu, Saru Kumari and Xiong Li, "A privacy-preserving and *provable* user authentication scheme for wireless sensor networks based on Internet of Things security", Journal of Ambient Intelligence and Humanized Computing, Springer, Volume 8, Issue 1, February 2017, Pages 101–116

[9] Peng Zhou, Siwei Jiang, Athirai Aravazhi Irissappane, Jie Zhang, Jianying Zhou and Joseph Chee Ming Teo "Towards Energy-Efficient Trust System through Watchdog Optimization for

WSNs", IEEE Transactions on Information Forensics and Security, Volume 10, Issue 3, March 2015, Pages 613 - 625

[10] Sarita Agrawal and Manik Lal Das, "Mutual Healing enabled Group-key Distribution Protocol in Wireless Sensor Networks", Computer Communications, Elsevier, Volume 112, November 2017, Pages 131-140

[11] Kakali Chatterjee, Asok De and Daya Gupta, "A Secure and Efficient Authentication Protocol in Wireless Sensor Network", Wireless Personal Communications, Springer, Volume 81, Issue 1, March 2015, Pages 17–37

[12] Li Sun, Pinyi Ren, Qinghe Du, and Yichen Wang "Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks", IEEE Transactions on Industrial Informatics, Volume 12, Issue 1, February 2016, Pages 291 – 300.