Received September 26, 2017, accepted October 22, 2017, date of publication November 3, 2017, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2770020

Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks

AMJAD MEHMOOD[1], AKBAR KHANAN[2,3], MUHAMMAD MUNEER UMAR[4], SALWANI ABDULLAH[2], KHAIRUL AKRAM ZAINOL ARIFFIN[2], AND HOUBING SONG[5], (Senior Member, IEEE)

[1]Institute of Information Technology, Kohat University of Science and Technology, Kohat 26000, Pakistan
[2]Centre for Artificial Intelligence Technology, Research Centre for Software and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Malaysia
[3]Department of Management Information System, A'Sharqiyah University, Ibra 400, Oman
[4]Department of Management and Information Technology, Jubail Industrial College, Jubail 31961, Saudi Arabia
[5]Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114 USA

Corresponding author: Amjad Mehmood (dramjad.mehmood@ieee.org)

This work was supported in part by the Ministry of Higher Education, Malaysia, under Grant FRGS/1/2015/ICT02/UKM/01/2 and in part by the Universiti Kebangsaan, Malaysia under Grant DIP-2016-024.

ABSTRACT Wireless sensor networks, due to their nature, are more prone to security threats than other networks. Developments in WSNs have led to the introduction of many protocols specially developed for security purposes. Most of these protocols are not efficient in terms of putting an excessive computational and energy consumption burden on small nodes in WSNs. This paper proposes a knowledge-based context-aware approach for handling the intrusions generated by malicious nodes. The system operates on a knowledge base, located at the base station, which is used to store the events generated by the nodes inside the network. The events are categorized and the cluster heads (CHs) are acknowledged to block maliciously repeated activities generated. The CHs can also get informational records about the maliciousness of intruder nodes by using their inference engines. The mechanism of events logging and analysis by the base station greatly affects the performance of nodes in the network by reducing the extra security-related load on them.

INDEX TERMS Intrusion detection system, knowledge base, cluster based WSN, security.

I. INTRODUCTION

The Wireless sensor networks (WSNs) are infrastructure-less, distributed and dynamic in nature [1]. The in richness capabilities of the WSN change to area of emergence technologies. Fog computing has an excellent example. In order to satisfying mobility support, geo distribution, locational awareness, and to low latency needs for the IoT applications, the Fog node facilitates the user in the execution of IoT applications [27].

Due to the vulnerable nature of WSNs, these networks are always exposed to severe types of threats which can vitiate their whole functionality. Authentication protocols and secure routing protocols implement the use of cryptographic keys to ensure secure transmission of data but cannot give protection against the inside attacks knows as passive attacks [10]. These protocols scramble. The valuable data from intruders who try to access them from outside, but a passive attack from a node inside cannot be avoided. According to Mehmood *et al.* [2], there are different types of possible attacks on WSNs like routing attacks, Sybil attacks and denial of service (DoS) etc.

Intrusion detection systems (IDS) can be used in WSNs to detect the suspicious behaviour of nodes inside the WSNs [3]. Cluster-based WSNs can reduce the performance load in terms of reducing the aggregate computation and energy consumption of all the nodes [4]. Due to technological development, WSNs have become visible and are used for various purposes in our daily life. Therefore, security in such networks is mainly focused on ensuring reliable performance of nodes in the network. IDS-based systems are very effective for detecting irregular actions of inner nodes of networks, preventing the whole network from various types of malicious attacks. The IDS agents will collect and analyze the abnormal behaviour of nodes in a time period and then apply appropriate actions. The work [5] has discussed various detection mechanisms for analysis. There are three possible ways of implementing IDS agents: centralized, distributed and hybrid. These agents are more efficient if installed at base stations, the centralized approach, because it does not affect the performance on small nodes in the network. According to [6], the term Situation Awareness (SA) is defined as the perception of some elements in the environment within a space and time period which can be used for projecting the near future. There are four levels of SA: perception, comprehension, projection and resolution [7].

Implementing security measurements on CHs (Cluster Head) in a cluster-based network is very beneficial due to its partially centralized approach for addressing prevention against various threats. The purpose of CHs is to collect knowledge on the nodes' behavior and to determine their s operation in the near future. The knowledge base in knowledge-based systems (KBSs) is used to gather and store data in symbolized form from various scenarios [8]. A knowledge base can be created for context awareness to overcome possible security threats from both internal and external intruders.

In our work, Knowledge-based IDS (KB-IDS) in a cluster-based WSN, we propose a technique for securing nodes by keeping a record of various behaviours of nodes inside the network.

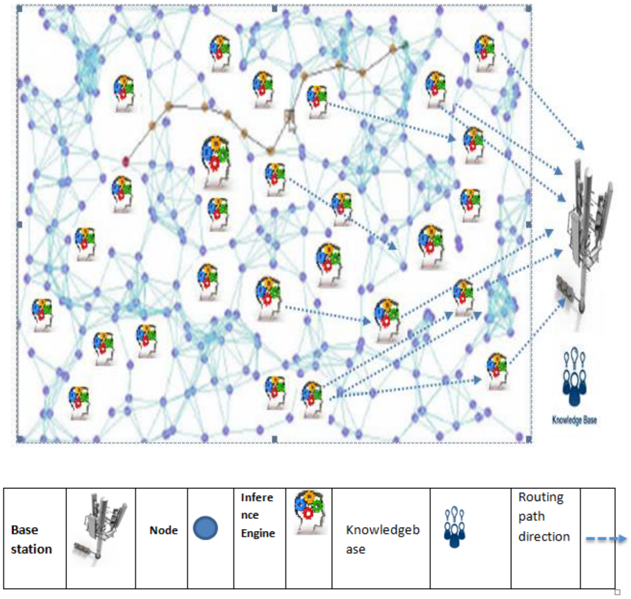


FIGURE 1. Cluster-based Intrusion Detection Mechanism for Smart Wireless Sensor Networks.

As shown in fig 1. the knowledge base may be bulky in size and requires lengthy computations, therefore it is stored on the base station. The CHs use inference engines to access the knowledge on behavior in the base station. They monitor the traffic and nodes behaviour, and generate events by sensing potential threats from the nodes using security context sensors. The events data is forwarded by the inference engines to the base station for further processing. The base station keeps, analyses, computes and concludes all the suspicious data provided. It is the responsibility of the base station to inform the CH about the maliciousness or non-maliciousness of a node after processing the behavioural data received. The CH, if it finds a malicious node, then blacklists the node by broadcasting its ID to all the member nodes.

The paper is organized as follows; Section II includes the related work done then section C explains our work on the KB-IDS; the simulation results are shown in section D and finally section E presents the conclusions.

II. RELATED WORK

Security threats to WSNs are dissimilar in nature from other wireless technologies. The biggest implication for the implementation of a security technique is the consideration of the constrained resources of nodes in the WSNs. Cryptographic techniques, in most cases, are considered as unsuitable for security implementation in WSNs [11]. Due to the broadcast transmission nature of the tiny nodes in the WSNs, they are always vulnerable to various kinds of attacks. Attacks on WSNs can be classified as either active or passive [10]. Active attacks directly affect the packet transmission and nodes performance in the network. These attacks can be DoS attacks, physical attacks, routing attacks and Sybil attacks etc. Meanwhile, passive attacks do not harm the performance or functionality of the network directly. These attacks include traffic monitoring, data packet reading and eavesdropping etc.

The IDS can be used to analyze the events and alerts generated by different nodes at various time periods [12] and [13]. It can be used for monitoring the current situation and estimating future predictions about the location and origin of the problem. To secure a wireless system, the functions of intrusion detection and then intrusion prevention are carried out [14]. In this process, all the events carried out by the nodes are noted and appropriate actions are taken upon detection of any activity by an intruder. Knowledge-based systems are problem-solving systems that keep the facts relating to a problem domain in a knowledge base for analysis and extraction of conclusions [15]. A knowledge base is a kind of database that stores facts and events data in the form of complex structures for manipulation and future predictions and problem-solving. This paper [18] proposes a method of creating a knowledge base for applying an evaluation system of network security.

Due to the centralized nature of cluster-based networks, it is more feasible to monitor the routes and traffic. In such networks, the nodes are grouped into clusters in such a way that each group is given a monitor node known as the cluster head (CH) [16]. CHs connect the base station, nodes inside their clusters and other CHs through direct or indirect routes. CHs monitor the behaviour of nodes and events generated inside their clusters [19]. CHs are selected in such a way that all the nodes inside their clusters benefit from their existence and all operations are monitored by them [20].

III. KNOWLEDGE BASED SECURE WSN SYSTEM

A considerable amount of work has been done in the area of securing WSNs from attacks through different approaches. Most of the proposed protocols are based on cryptographic techniques. Such protocols impose a substantial load on the nodes of a WSN due to their limited resources and computational capabilities [24]. Naranjo *et al.* [26] proposed a technique to organize node, and select the CHs in WSNs. The technique proposes two level energy for the normal and advanced. The technique show fair for the selection of CH with having same probability to select.

Zhang *et al.* [21] proposed an authentication system for low-powered nodes. The nodes pass a packet for mutual authentication. In the proposal an elliptic curve cryptosystem-based trust procedure is generated. The work claims to provide protection against both active and passive attacks. The base station also involves the authentication process for nodes. Umar *et al.* [22] proposed a novel message observation mechanism (MoM) to find and avoid DoS attacks. Reference [23] focused on the conclusions that a system reconsiders to make new detections of attacks. However, such schemes have their own limitations. Most of the work has been done on optimizing the process of detection rather than prevention of future attacks. Chen [17] proposed a scheme having two stages of offline training and online testing. In the offline training stage, samples of features are extracted to train the models. In the online testing stage, the network packets are captured and then compared with the training models to detect the intrusions in the network. The DISSN [25] applies a dynamic robust security framework in the context of shared sensor networks. The proposed work uses a Byzantine algorithm for monitoring and collaboration of the nodes neighbourhood to enhance the security of the system by identifying attacks. Naranjo *et al.* [26] presented interactive linear systems to handle repeated attacks. The values of these systems are represented by transmitted messages. These values are considered for tackling the threads generated by intruders.

IV. KB-IDS IN CLUSTER-BASED WSNs

In our work, KB-IDS, the network is divided into clusters in such a way that each cluster is given a CH. The CH monitors the behaviour of all its member nodes inside its cluster. The behavioural data is recorded in the form of unique events. Each event consists of an ID, invoke time, type, attack-ID and source and destination IDs of nodes. These events are transferred to the base station. The base station performs various functions on the stored events received in order to lessen the load on the CH and the number of effective events. Redundant events and those that were caused by some network condition and not by intruders are eliminated by the base station:

$$Ei = [Ty, t, Attack\_ID, Source\_ID, Dest\_D]$$

where Ty is the type of event generated at the time t and i is the event ID from 1 to n. By analyzing different events, we can get unique simplified events Em:

$$Em \to if\ Ei = Ej, \quad for\ each\ i = 1\ to\ n\ and\ j = 1\ to\ n.$$

Once the base station has stored enough events information in its knowledge base, it provides assistance to the CHs to determine the maliciousness of operations carried out by the member nodes. The cluster nodes can infer, using their inference engines, the knowledge base on the base station about the details on an event. Knowledge discovery through the Frequent Pattern (FP) mining algorithm [9] is done at the base station to check the status of the event. If the system does not find the provided event, it stores it for further processing, or if the event information is available, the base station provides the conclusion to the CH for that event. The conclusion indicates the status and type of event, from which the CH can determine the suspiciousness of the nodes involved. Once the CH concludes the maliciousness of a node, it identifies the said node as blacklisted and broadcasts this information throughout its cluster.

The whole process can be explained in the following steps:

Step 1: The sensor nodes are installed in the network and grouped together into clusters according to their locations and similarities.

Step 2: CHs are selected among the nodes in the respective clusters under some criteria.

Step 3: A blank knowledge base is installed on the base station.

Step 4: The CHs are provided with the inference engines for using the knowledge base on the base station.

Step 5: The CHs monitor all the node-related events and data transmission in their clusters in such a way that all the nodes communicate through their CH, directly or indirectly.

Step 6: The monitored data is considered as events and sent to the knowledge base on the base station.

Step 7: The base station analyzes the data to determine the suspiciousness of events.

Step 8: The base station eliminates redundant and routine events from the base station.

Step 9: The CHs are acknowledged about the routine events so that they will not consider such events in future.

Step 10: The base station alerts the CHs about the pattern of threat events. The CHs take action upon such alerts.

Step 11: The CHs, upon receiving suspicious alerts, blacklist the generating nodes and broadcast the information to their member nodes.

Step 12: The CH may report some unknown event due to network conditions which are analyzed at the base station. Such events are eliminated and the CHs become aware so as not to report such events again.

Step 13: Due to overload on the CHs, they may exhaust their energy very soon. A CH control is switched to another node upon consumption of energy to a specified limit.

It is not necessary for only single events to be considered for judging and conclusion. A specific set or pattern of events can also involve an attack by intruders. The tree mechanism is used to determine the occurrence of patterns of events.

TABLE 1. Patterns of events.

Pattern ID	Events	Involved Nodes	Type
1	E1,E11,En,E3	Source=N1 and Dest=Nn	Safe
2	E19,E11,E2	Source=N10 and Dest=N2	Unsafe
3	E1,E11,E2,E19	Source=N1 and Dest=Nn	Safe
4	E5,E15,En	Source=N10 and Dest=N5	Unsafe
5	E7,E2,E3,E1	Source=N2 and Dest=N1	Unsafe
6	E7,E2,E7	Source=N10 and Dest=N2	Unsafe
7	E19,E11,E2	Source=N4 and Dest=Nn	Safe
8	E7,E2,E3,E1	Source=N13 and Dest=N2	Safe
9	E3,E4,E7,E6	Source=N15 and Dest=Nn	Safe
10	E11,En,En,En	Source=N3 and Dest=N2	Safe

TABLE 2. Simulation parameters.

Parameter	Value
Number of nodes	80
Number of clusters	3
Nodes per cluster	20 – 40
Number of malicious nodes	8
Routing	Adhoc
Area	100 * 100 m
Antenna type	Omni
Mac type	802.11
Number of base stations	1

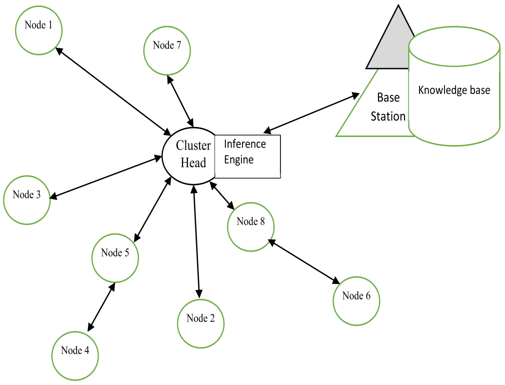


FIGURE 2. The System.

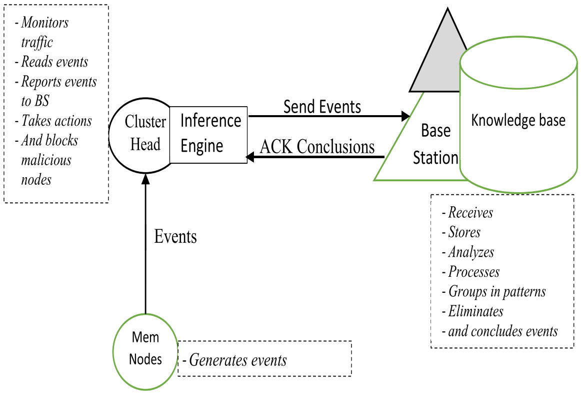


FIGURE 3. Events handling and operations.

The system records a stated number of events to form a pattern. If the recorded pattern does not appear suspicious, then it is considered as ''safe''; otherwise, the pattern is labeled as ''unsafe''. The CH within a specified time interval tracks the events and forwards them to the base stations for verification. Table 1 shows the patterns of events.

A few things need to be considered in the table above. Some events and nodes are indicated with an 'n', where n indicates the generic node and can be used with any number. The table shows two suspicious nodes, number 2 and number 10, with different activities sets. Pattern ID 1 and pattern ID 7 have the same events but different types due to the involvement of different nodes.

V. SIMULATION RESULTS

The work has been simulated in NS 2.35 under the Ubuntu operating system. A wireless network of 80 nodes, divided into 3 clusters, is created. Each cluster is assigned 2 to 3 malicious nodes. Some of the simulation parameters are as follows in Table 2.

The attacker nodes continuously generate ICMP pings to initiate DDos attacks. The cluster nodes monitor these activities and forward these events to the base station.

The performance of the developed system is checked by changing the number of nodes. The simulation results are as (a) the work load on the CH as compared to the member nodes, (b) the number of nodes versus packet delivery ratio, (c) the number of nodes compared to average end-to-end delays, (d) the number of nodes versus throughput, (e) average energy consumption, (f) and the effectiveness of our work against non-secured routing.

Figure 3 shows the average load on member nodes compared to the load on the CHs, recorded at different time intervals. As the CHs use inference engines along with the traffic monitoring, they therefore take extra load. Once the system is established and the knowledge base is updated with new events, then the load becomes uniform as shown in the figure.

In Figure 4, the packet delivery ratio in percentage of our system is compared with a routine system. The delivery rate is relatively high due to non-usage of heavy cryptographic algorithms and other security measurements. The delivery rate increases as the system learns with an increased number of nodes, while the other non-KB-IDS system decreases its

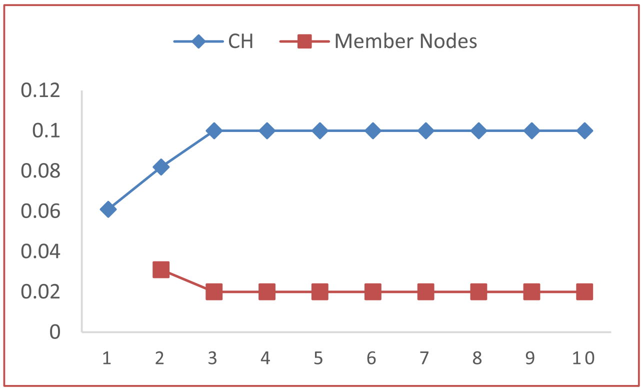


FIGURE 4. Workload on cluster head versus member nodes.

performance due to the increased load of the enlarged number of nodes.

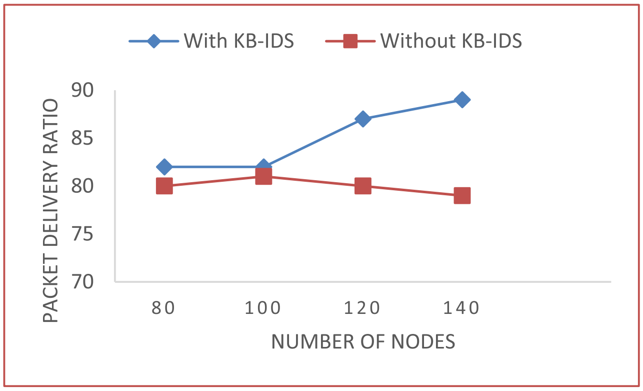


FIGURE 5. Number of nodes versus packet delivery ratio.

From Figure 5, it is observed that our system gives a maximum value of 0.003, while the other system has much higher values starting from 0.03 to 0.05. Hence the end-to-end delay is considered less in the knowledge-based system than in other systems in Figure 6.

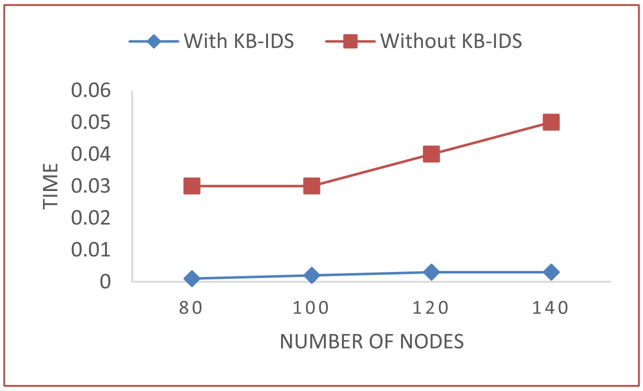


FIGURE 6. Number of nodes compared to average end-to-end delays.

The throughput of KB-IDS is better than the systems that do not use knowledge bases. The application of KB-IDS supports effective network security and overcomes the drawbacks of the existing security controls. Malicious attackers are detected and blocked by the CHs through the reporting of events to the base station in Figure 7.

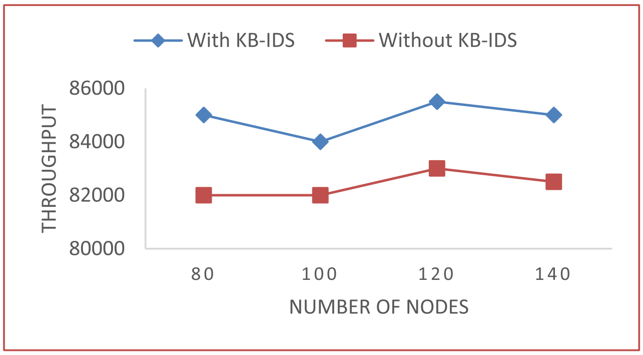


FIGURE 7. Number of nodes versus throughput.

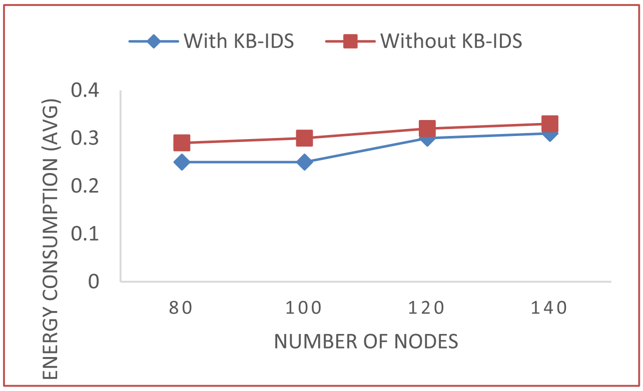


FIGURE 8. Average energy consumption.

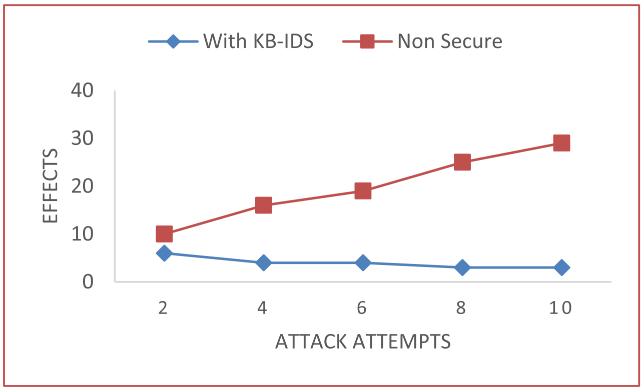


FIGURE 9. Effectiveness versus non-secured routing.

Because it requires less processing and computation by the nodes in the network, the KB-IDS consume less power on average by all the nodes in aggregate (see Figure 2).

KB-IDS is more secure against attacks as it stores the events which are used for generating malicious attacks. The graph in Figure 8 shows a decrease in the effectiveness of attacks with the increasing number of attack attempts due to the maintenance of the knowledge base. The systems learn from the events and prevent intruders and malicious attacks happening again in future (see Figure 9).

VI. CONCLUSION

Our system, KB-IDS, primarily focuses on the analysis of events generated by different nodes in a WSN. The events are stored in a knowledge base located at the base station. The whole network is divided into a number of clusters and in each cluster a node is nominated as the head. The CHs communicate with the base station and forward events data to the knowledge base through inference engines. The system is quite effective as it does not use heavy security algorithms that put an additional computation and storage load on all the nodes inside a network. KB-IDS puts a load on a single node inside the cluster. More importantly, the traffic is monitored and any suspicious event generated by an attacker node is blocked by the CHs due to storing knowledge about the nature of events. For increasing the performance of the proposed system, the events are also processed and grouped into different patterns. The system also supports the switching of CHs with other member nodes whenever needed. The KB-IDS showed reasonably acceptable simulation results compared to other security and non-security systems. This approach can be further expanded by distributing the load of the CH on all the nodes. The knowledge and events processing can be handled by advanced computational algorithms.

REFERENCES

[1] A. Mehmood, S. Khan, B. Shams, and J. Lloret, "Energy-efficient multi-level and distance-aware clustering mechanism for WSNs," *Int. J. Commun. Syst.*, vol. 28, no. 5, pp. 972–989, 2015.

[2] A. Mehmood, J. Lloret, and S. Sendra, "A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring," *Wireless Commun. Mobile Comput.*, vol. 16, no. 17, pp. 2869–2883, 2016.

[3] A. Mehmood, M. M. Umar, and H. Song, "ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks," *Ad Hoc Netw.*, vol. 55, pp. 97–106, Feb. 2017.

[4] V. Patel and J. Gheewala, "An efficient session key management scheme for cluster based wireless sensor networks," in *Proc. IEEE Int. Adv. Comput. Conf. (IACC)*, Jun. 2015, pp. 963–967.

[5] M. M. Umar, A. Mehmood, and H. Song, "A survey on state-of-the-art knowledge-based system development and issues," *Smart Comput. Rev.*, vol. 5, no. 6, pp. 498–509, 2015.

[6] A. Mehmood, H. Song, and J. Lloret, "Multi-agent based framework for secure and reliable communication among open clouds," *Netw. Protocols Algorithms*, vol. 6, no. 4, pp. 60–76, 2014.

[7] T. Bass, "Multisensor data fusion for next generation distributed intrusion detection systems," in *Proc. Net. Symp. Draft*, 1999, pp. 24–27.

[8] D. J. Power, R. Sharda, and F. Burstein, *Decision Support System*. Hoboken, NJ, USA: Wiley, 2015.

[9] S.-H. Liao, P.-H. Chu, and P.-Y. Hsiao, "Data mining techniques and applications—A decade review from 2000 to 2011," *Expert Syst. Appl.*, vol. 39, no. 12, pp. 11303–11311, 2012.

[10] A. Wahid and P. Kumar, "A survey on attacks, challenges and security mechanisms in wireless sensor network," *Int. J. Innov. Res. Sci. Technol.*, vol. 1, no. 8, pp. 189–196, 2015.

[11] A. Alam and D. Eyers, "Securing WSN update from intrusion using time signature of over the air update protocol," in *Proc. 13th Australasian Symp. Parallel Distrib. Comput. (AusPDC)*, 2015, pp. 107–110.

[12] A. Mehmood, A. Khanan, A. H. H. M. Mohamed, and H. Song, "ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET," *IEEE Access*, to be published, doi: 10.1109/ACCESS.2017.2732727.

[13] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.

[14] A. F. Serpella, X. Ferrada, R. Howard, and L. Rubio, "Risk management in construction projects: A knowledge-based approach," *Proc.-Soc. Behavioral Sci.*, vol. 119, pp. 653–662, Mar. 2014.

[15] M. M. Umar, A. Mehmood, and H. Song, "SeCRoP: Secure cluster head centered multi-hop routing protocol for mobile ad hoc networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3378–3387, 2016.

[16] S. Wang, Q. Li, and Y. Guo, "A novel intrusion detection method for WSN," in *Proc. STA*, vol. 1. 2015.

[17] M. Chen, "A study on the generation method of knowledge base rules of network security evaluation system," *J. Changchun Normal Univ.*, vol. 3, p. 13, 2012.

[18] N. Gupta, M. Shrivastava, and A. Singh, "Cluster based on demand routing protocol for mobile ad hoc network," *Int. J. Eng. Res. Technol.*, vol. 1, no. 3, pp. 1–5, 2012.

[19] M. Singh and S. Gagangeet, "A secure and efficient cluster head selection algorithm for MANET," *J. Netw. Commun. Emerg. Technol.*, vol. 2, no, 2, pp. 49–53, 2015. [Online]. Available: https://www. jncet.org

[20] J.-Z. Lu and J. Zhou, "On the security of an efficient mobile authentication scheme for wireless networks," in *Proc. 6th Int. Conf. Wireless Commun. Netw. Mobile Comput. (WiCOM)*, 2010, pp. 1–3.

[21] Y.-Y. Zhang, X.-Z. Li, and Y.-A. Liu, "The detection and defence of DoS attack for wireless sensor network," *J. China Univ. Posts Telecommun.*, vol. 19, pp. 52–56, Oct. 2012.

[22] M. M. Umar, N. Alrajeh, and A. Mehmood, "SALMA: An efficient state-based hybrid routing protocol for mobile nodes in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2016, Jan. 2016, Art. no. 3.

[23] E. S. Kumar, "Random keying technique for security in wireless sensor networks based on memetics," *Int. J. Comput. Sci. Theory Appl.*, vol. 1, no. 2, pp. 25–31, 2014.

[24] C. M. de Farias, R. Pinheiro, R. O. Costa, and I. L. dos Santos, "DISSN: A dynamic intrusion detection system for shared sensor networks," *Autom. A J. IFAC, Int. Fed. Autom. Control*, pp. 348–357, 2014. [Online]. Available: https://www.journals.elsevier.com/automatica/

[25] S. Sundaram, S. Revzen, and G. Pappas, "A control-theoretic approach to disseminating values and overcoming malicious links in wireless networks," *Automatica*, vol. 48, no. 11, pp. 2894–2901, 2012.

[26] P. G. V. Naranjo, M. Shojafar, H. Mostafaei, Z. Pooranian, and E. Baccarelli, "P-SEP: A prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks," *J. Supercomput.*, vol. 73, no. 2, pp. 733–755, 2017.

[27] I. Ullah *et al.* (2017). *Telecommunication Systems*. [Online]. Available: https://doi.org/10.1007/s11235-017-0352-x

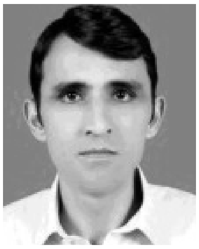
AMJAD MEHMOOD received the Ph.D. degree in wireless networks from the Kohat University of Science and Technology, Kohat, in 2014. He received the virtual Post-Doctoral Fellowship from the University of Virginia, USA. He is currently pursuing the Post-Doctoral degree with the Guangdong Provincial Key Laboratory on Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, Maoming, China. Since 2003, he has been a Senior Faculty Member and a Coordinator of different programs with the Institute of IT, Kohat University of Science and Technology.

He is interested in the areas of cyber-physical systems, IoT, connected vehicles, wireless communications and networking, optical communications and networking, smart grid communications and networking, security issues in wireless networks, big data, cloud computing, and fault diagnosis in wireless sensor networks. He has supervised many B.C.S., M.C.S., M.S., and Ph.D. students in the abovementioned fields. He was involved with reviewing and organizing different workshops, seminars, and training sessions on different technologies. He has authored over 50 academic articles in reputed peer-reviewed international journals and conferences around the world.

He has been serving as a TPC Member, a Reviewer, the Publication Chair, the Poster Chair, and the Demo Chair for numerous international conferences, including CCNC, SCPA, WICOM, INFOCOM, and SCAN. He serves as a Reviewer or an Associate Editor for many peer-reviewed international journals.

AKBAR KHANAN received the master's degree in computer science from the Kohat University of Science and Technology, Kohat, in 2011. He is currently pursuing the Ph.D. degree from the University Kebangsaan Malaysia, Bangi, Malaysia. Since 2012, he has been a full time Faculty Member and a Coordinator of different programs with the Department of Management Information System, College of Business Administration, A'Sharqiyah University, Ibra, Oman.

He was a Supervisor of many graduate and undergraduate students with the College of Business Administration. He has also been involved organizing different workshops, seminars, and training sessions. He is interested in the areas of IoT, connected vehicles, wireless communications, and networking, security issues in wireless networks, big data, cloud computing, and smart cities. He has a special interest in quality auditing (Q.A) and served many Q.A activities including self-review auditing etc.



MUHAMMAD MUNEER UMAR is currently pursuing the Ph.D. degree in computer science with the Kohat University of Science and Technology, Pakistan. He is currently a Lecturer in computer science with Jubail Industrial College, Saudi Arabia. He has authored some research articles in reputable journals. His research work is in the areas of security and routing protocols for MANETs and WSNs.

SALWANI ABDULLAH received the B.Sc. degree in computer science from the Universiti Teknologi Malaysia, the master's degree in computer science from the Universiti Kebangsaan Malaysia (UKM), and the Ph.D. degree in computer science from the University of Nottingham, U.K. She is currently a Professor in combinatorial optimisation with the Faculty of Information Science and Technology, UKM. Her research interests include artificial intelligence and operation research, particularly in meta-heuristic algorithms in optimisation areas that involve different real world applications in static and dynamic optimisation problems, such as university timetabling, job shop scheduling, nurse rostering, space allocation, and data mining tasks.

KHAIRUL AKRAM ZAINOL ARIFFIN received the bachelor's and master's degrees (Hons.) in System Engineering with Computer Engineering from the University of Warwick, U.K., in 2008 and 2009, respectively. He joined the Universiti Teknologi PETRONAS in 2010 to pursue his journey towards academic research and teaching courses to earn the Ph.D. degree in information system. He has authored a number of journal articles and conference papers and published internationally. He was a Researcher with the Digital Forensic Department, CyberSecurity, Malaysia, and had been entrusted with the research on embedded system. He is currently a member with the Technology and Information Science Faculty, The National University of Malaysia to pursue his passion in research towards algorithms, embedded system, image processing and audio authentication. He is a GCFA certified and a member of the IET.

HOUBING SONG (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012.

He was with the Faculty of West Virginia University from 2012 to 2017. In 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA. In 2007, he joined the Texas A&M Transportation Institute as an Engineering Research Associate. He is currently an Assistant Professor and the Director with the Security and Optimization for Networked Globe Laboratory (SONG Lab), Embry-Riddle Aeronautical University. He has authored over 100 articles. He is the Editor of four books, including *Smart Cities: Foundations, Principles and Applications* (Wiley, 2017); *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications* (Wiley-IEEE Press, 2017); *Cyber-Physical Systems: Foundations, Principles and Applications* (Academic Press, 2016); and *Industrial Internet of Things: Cybermanufacturing Systems* (Springer, 2016). He serves as an Associate Technical Editor of the *IEEE Communications Magazine*. His research interests include cyber-physical systems, cybersecurity and privacy, Internet of Things, edge computing, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking.

Dr. Song is a Senior Member of ACM. He was a very first recipient of the Golden Bear Scholar Award, the highest campus-wide recognition for research excellence at West Virginia University Institute of Technology, in 2016.