International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.401-410
http://dx.doi.org/10.14257/ijsia.2014.8.1.37

Sinkhole Vulnerabilities in Wireless Sensor Networks

Junaid Ahsenali Chaudhry[1], Usman Tariq[2], Mohammed Arif Amin[3] and Robert G. Rittenhouse[4]

[1]Center for Advanced Image and Information Technology,
School of Electronics & Information Engineering,
ChonBuk National University,
Jeonju, Korea.
[2]College of Computer Engineering & Sciences
Salman Bin Abdulaziz University
151 Alkharj 11942 Kingdom of Saudi Arabia
[3] Department of Computer and Information Science (HCT),
Abu Dhabi, United Arab Emirates.
[4]Keimyung Adams College, Keimyung University
Daegu, 704-701, South Korea,
writetochaudhry@gmail.com u.tariq@sau.edu.sa marifamin@gmail.com,
rrittenhouse@acm.org (corresponding author)

Abstract

Sinkhole attacks in wireless sensor networks occur when a compromised node tries to attract network traffic by advertising un-authorized/illegitimate routing updates. The victim node sends data to the compromised node rather than sending it to the node it was formerly using. Sinkhole attacks are typically used to launch other attacks on the network such as selective forwarding and wormhole attacks. Once the network is compromised it is very hard to predict the kind of attack that is to follow. For this reason, there is a need to strengthen the security of wireless sensor networks. In this paper, we first describe the challenges in detecting sinkhole attacks in wireless sensor networks, followed by an analysis of methods to prevent, detect and neutralize sinkhole attacks. The analysis will be based on discussing the advantages and limitations of the proposed solutions.

Keywords*: Intrusion detection, Sinkhole attack, wireless sensor networks*

1. Introduction

Wireless sensor networks (WSNs) are composed of small sensor units able to sense and send data to base stations via an ad hoc mesh network established as the sensors are deployed [1]. Applications include deployment by the military to track enemy movement, environmental monitoring such as fire detection and health services such as cardiac monitoring [2-4]. Unfortunately many WSNs are deployed in unfriendly areas and are often left unattended. In addition, most routing protocols used in WSNs do not consider security aspects due to resource constraints of the sensors including low computational power, limited memory, small power supplies and limited communication range [5, 6]. This creates opportunities for attackers. Sinkhole attacks are typical of such attacks. A sinkhole attack is a network layer attack where an adversary tries to attract traffic with the aim of preventing the base station from

ISSN: 1738-9976 IJSIA

receiving complete and correct sensing data from nodes [7]. The intruder compromises or inserts a node relatively close to the base station and uses it to launch an attack. The compromised node sends fake presence and routing information to neighboring nodes about its link quality which is used by the routing metric to select the best route for data transmission. This results in all the traffic from the compromised node's neighbors passing through it to the base station [8]. Other attacks such as the selective forward attack, altered routing information attack and knowledge spoofing attack can use a sinkhole attack as a springboard [4]. A sinkhole attack can also be used to send bogus information to the base station. A variety of different methods have been proposed to detect and counter sinkhole attacks [9]. This paper surveys and reviews these solutions.

2. Sinkhole Attacks

In a sinkhole attack an intruder compromises an existing node or introduces a counterfeit node inside the network and uses it to launch an attack. The attacker node tries to attract all the traffic from neighboring nodes based on the routing metric used in the routing protocol. When the attacker node manages to attract neighboring nodes, it becomes a sinkhole and can be used to launch other attacks. Sinkhole attacks are a form of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself [10]. Due to the ad hoc network setup and many to one communication pattern of wireless sensor networks, where many nodes send data to a single base station, WSNs are particularly vulnerable to sinkhole attacks [11]. Based on the communication flow in the WSN the sinkhole does not need to target all the nodes in the network but only needs to target nodes close to the base station.

Figure 1Figure 1a shows the network structure before a sinkhole attack. Here Node 3 can communicate to base station through either Node 1 or Node 2 and selects Node 2 because it yields the shortest path to the base station.

In Figure 1b Node 1 has been compromised and now announces a false shorter path to the base station. This causes Node 3 to route its communication to the base station through Node 1.

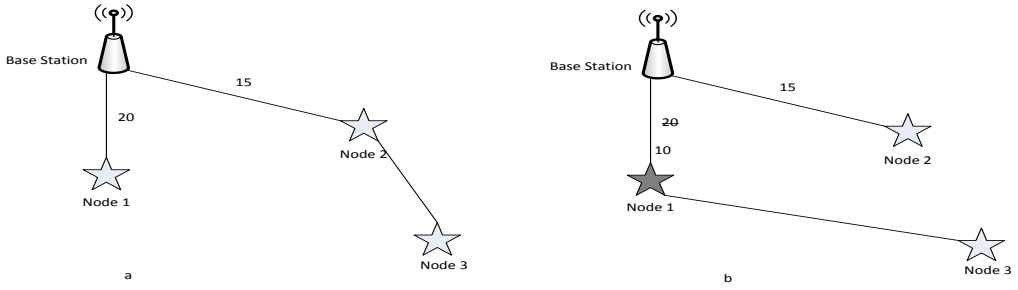


Figure 1. Sinkhole Attack

We consider two particular scenarios of sinkhole attacks. In the first the intruder has more power than other nodes. In the second the intruder and other nodes have the same power. In both cases the intruder claims to have the shortest path to base station so that it can attract network traffic. In a wireless sensor network the best path to the base station is the basic metric for routing data

In Figure 2a the intruder has greater computational and communication power than other nodes and has managed to create a high quality single hop connection with the base station. It then advertises its high quality routing message to its neighbors. After that all the neighbors will divert their traffic to the base station to pass through the intruder and the sinkhole attack is launched. Note that the sinkhole will not generally be able to capture sensors adjacent to the base station.

In Figure 2b the sinkhole is not more powerful than the other nodes. As a consequence it is only able to cause the nodes "nearby" to change their routing. Note that if the sinkhole in this scenario were to advertise a path shorter than that of the node it is using to communicate with the base station it would capture that node and prevent the captured nodes from communicating with the base station at all. The sinkhole would then function as a black hole and be more easily detected.

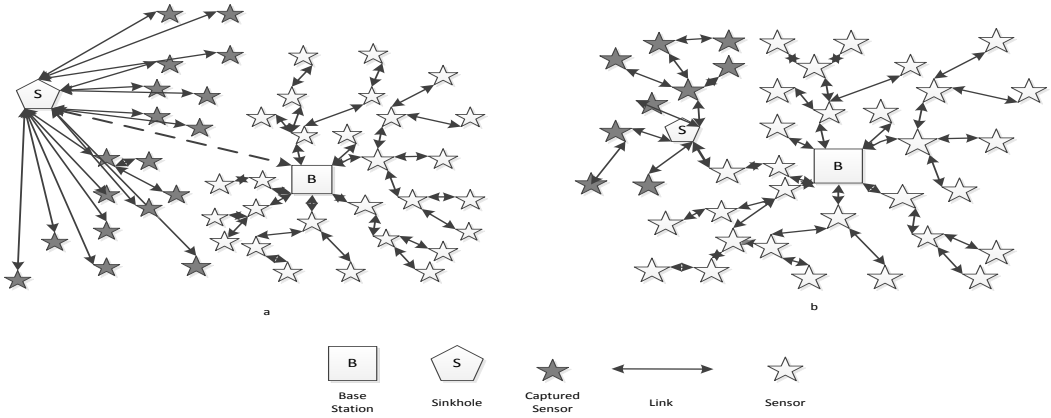


Figure 2. Example Sinkholes

3. Challenges in Detecting Sinkhole Attacks in WSN

Based on our review of the literature on sinkhole attacks in WSNs, the following are the main challenges in detecting sinkhole attack in wireless sensor networks:

i. *Communication patterns in WSNs:* All the messages from sensor nodes in a WSN are destined for the base station but often routed through other nodes creating an opportunity for a sinkhole to launch an attack. Based on that communication pattern the intruder need only compromise nodes close to the base station instead of targeting all nodes in the network. This is a challenge because the communication pattern itself provides the opportunity for attack.

ii. *Dynamic nature of WSN:* Sensor networks are ad hoc networks with routing patterns built as sensors and base stations come online. Low power wireless signals are subject to sporadic interference. Sensors may not be optimally placed for communications, may not be always on and may, in some cases, move.

iii. *Specific sinkhole attacks depend on routing protocols:* In WSNs packets are transmitted based on a routing metric which varies for different routing protocols [12]. For example the techniques used by a compromised node in network that uses the TinyAODV protocol will be different from the one used another protocol such as the MintRoute protocol. However, these protocols are generally based on how "close" a node is to the base station. An attacking node can exploit this to lie to its

neighbors in order to launch a sinkhole attack. Then all the data from its neighbors to the base station will pass through the attacker node.

iv. *Sinkhole attacks may be insider attacks;* Insider and outsider attacks are two categories of attacks on networks. An outsider attack adds a malicious node to the network. In an insider attack the intruder compromises one of the legitimate nodes by tampering with it or through weakness in the victim's system software; compromised nodes inject false information in the network or listen to secret information. A compromised node possesses adequate access privilege in the network and already has knowledge pertaining to the network topology which creates additional challenges in detection. Due to this situation, even cryptography may not entirely defend against insider attack [8]. Therefore insider attacks pose a more serious threat to systems than outsider attacks.

v. *Resource constraints limit detection methods:* The limited power supply, low communication range, low memory capacity and low computational power of sensors are the main constraints in WSNs that hinder implementation of strong security mechanisms. The strong cryptographic methods used in other networks cannot be implemented in a WSN due to low computational power and low memory capacity. Therefore weaker methods compatible with available resources must be used.

vi. *Vulnerability to physical attack:* A wireless sensor network may be deployed in a hostile environment and left unattended. This provides an opportunity for an intruder to attack a node physically and get access to all necessary information [13].

vii. *Vulnerability to key compromises:* An adversary may be able to crack the authentication key stored inside the sensor node. It may also be possible to reverse engineer the chipset, locate the key and crack it or use brute-force methods.

4. Related Work

Due to resource constraints traditional security mechanisms are not applicable to a WSN. Different researchers have proposed different solutions to detect and identify sinkhole attacks in wireless sensor networks. This section discusses these solutions.

4.1. Categorizing Existing Approaches

Existing approaches may be divided into methods to prevent sinkholes from occurring and methods to detect sinkholes after they appear [14]. Prevention approaches are more difficult to achieve due to the lack of computational power in the sensors. Some researchers have proposed hybrid systems combining both methods.

Detection: in detection approaches normal user behavior is defined and the intrusion detection strategy is to search for anything that appears anomalous in the network. In this method intrusion is considered as anomalous activity because it looks abnormal compare to normal behavior. Rule based and statistical approaches are a subset of anomaly based detection approaches [15].

Rule based: In the rule based approach rules are designed based on the behavior or technique used to launch sinkhole attacks. These rules are implanted in intrusion detection system running on each sensor node or on specialized monitors [16]. Packets transmitted through the network by nodes are then analyzed according to these rules and any node will be considered an adversary and isolated from the network if it violates the rules.

Statistical: In the statistical approach data associated with certain activities of the nodes in network is studied and recorded. For example, the network could monitor the normal packet

transmission patterns between the nodes or monitor resource depletion of the nodes such as CPU usage. Then the adversary or compromised node can be detected by comparing the actual behavior with the threshold value which used as reference, any node exceeding that value is considered an intruder.

Prevention: In this approach the integrity and authenticity of packets traveling within the network is protected by using encryption and decryption keys. Any packet transmitted in the network is encrypted such that to access that message requires a key and any small modification of the message can be easily detected.

Hybrid: The combination of both anomaly and cryptographic approaches is used in this approach. The false positive rate produced by anomaly based methods is reduced in this approach due to the use of both methods [17]. Another advantage of this approach is being able to catch any suspicious nodes when their signature is not included in detection database.

4.2. Detection Based Approaches

Krontiris *et al.,* used a distributed rule based detection system to detect sinkholes [18]. Their system runs on all individual sensor nodes. Two rules are implemented in the intrusion detection system. An alarm is sent by the intrusion detection system when either one of the rules is violated by one of the nodes but it does not provide the node ID of the compromised node. The two rules are: "*For each overhead route update packet check the sender field, which must be different than your node ID. If this is not the case, produce an alert and broadcast it to your neighbors."* and "*For each overhead route update packet check the sender field, which must be the node ID of one of your neighbors. If this is not the case, produce an alert and broadcast it to your neighbors."* A collaborative approach can then be used to identify and exclude the sinkhole.

In later work Krontiris, Giannetsos and Dimitriou used a similar rule based approach [19]. Their two rules were: "*For each overheard route update packet, check the sender field, which must belong to one of your neighbors"* and "*For each [parent, child] pair of your neighbors, compare the link quality estimate they advertise for the link between them. Their difference cannot exceed 50.*" While this approach will not by itself identify the sinkhole, extension to a collaborative approach should.

Tumrongwittayapak and Varakulsiripunth proposed a system that uses the RSSI (Received Signal Strength Indicator) value with the help of extra monitor (EM) nodes to detect sinkhole attacks [15, 16]. EM nodes have greater communication ranges than standard nodes. One of their functions is to calculate the RSSI of nodes sending packets and send it to the base station with the ID of source and next hop. This process happens instantly when nodes are deployed. The base station uses that value to calculate a VGM (visual geographical map). That VGM shows the position of each node and later when the EM sends updated RSSI values and the base station identifies a change in packet flow from previous data a sinkhole attack can be detected. The compromised node is identified and isolated from the network by the base station using the VGM value. However if an attack is launched immediately after network deployment the system will not be able to detect it [20]. In addition the numbers of EM nodes were not specified for specific numbers of sensor nodes and the solution focused only on static networks [16].

Sheela, Kumar and Mahadevan proposed a non-cryptographic method using mobile agents to defend against sinkhole attack. The mobile agents create an information matrix of each node by analyzing data transfer. Those information matrixes prevent wireless sensor nodes from believing the false path from sinkhole node. However the

proposed solution creates high network overhead when the number of nodes increases. Also the complexity of storing an information matrix at every node reduces the efficiency of the proposed solution [21].

Roy *et al.,* proposed a Dynamic Trust Management system to detect and eliminate multiple attacks such as sinkhole attacks [12]. Each node calculates the trust of its neighbor node based on experience of interaction; recommendation and knowledge then sends it to the base station. The base station decides which node is a sinkhole after it receives several trust values from other nodes. When the trust value of a node falls below the normal value of 0.5 it is considered a sinkhole attack node. Simulations show sinkholes being quickly detected and eliminated [12].

Mathews *et al.,* describe an anomaly based intrusion detection algorithm used to detect compromised sensor nodes. The algorithm uses packet arrival time to differentiate between a legitimate and the suspicious node. Sensor nodes keep track of a number of packet arrival and transmission times. If a sensor node sends a packet with an arrival time inconsistent with previous entries for that node the base station is notified. The base station then requests the packet transmission time entries from the suspicious node. If these do not correspond to the arrival times reported the node is marked as compromised and excluded from the network [22].

In [23] changes in neighboring nodes and the power levels received from neighboring nodes is used to identify potentially compromised nodes. This work assumes that a node is removed from the network, compromised and then redeployed in a different location.

In [24], a behavior-based approach is presented to detect a compromised sensor node. The method assumes that each node can observe behavior of another node and that messages sent are encrypted using keys. If any node's behavior changes then it is considered to be compromised. The method assumes that the network is static and all the nodes do not change any parameters including location after installation.

[25] Presents an intrusion detection system that can detect multiple attacks. The system is installed on sensors throughout the network and keeps track of numbers of packets sent, received, forwarded and retransmitted by neighbor nodes. Sinkholes can be detected by observing an abnormally high number of received packets. Threshold values are set by simulation prior to actual network deployment.

A hop count based system is presented by [26] in which advertised hop count values are monitored for significant changes. The scheme employs an Anomaly Detection System (ADS) deployed on specialized nodes throughout the WSN. The scheme is able to detect sinkholes with a high degree of accuracy when the ADS nodes are properly located.

Onat and Miri developed an anomaly based detection method to find the compromised nodes in the network using the neighbor table and node based statistics gathering and analysis. Their method assumes that every node in the network has a unique identifier, that the network is stable in that new nodes do not appear and that nodes do not change location or transmission power levels. Each node tracks packet arrival rate and received power from neighbor nodes. Variations from the normal pattern can then be used to identify an intruder [14]. This technique is not applicable if the assumptions about the network do not hold.

Ngai, Liu and Lyu proposed a statistically based intruder detection algorithm to protect against sinkhole attacks in wireless sensor networks. The proposed algorithm has two steps. The first step is using data consistency to locate the list of suspect nodes and the second is to identify the intruder through analyzing the network flow information. Their algorithm involves the base station in the detection process. The

results show the accuracy rate is good and the method has low communication overhead [11].

Chen, Song and Hsieh proposed a GRSh (Girshick-Rubin-Shyriaev)–based algorithm, essentially a statistical algorithm, for detecting compromised nodes in wireless sensor networks [2]. In this solution the data associated with certain resources or activities of the nodes are collected and analyzed. Then that value (threshold) is established and used as a reference to detect a malicious or compromised node in the network. In this solution the difference of CPU usage of each node is calculated by the base station after monitoring CPU usage of each node for a fixed time. Then the node can be identified as a malicious node by the base station after comparing the difference with a threshold value.

4.3. Prevention Based Approaches

Sharmila and Umamaheswari proposed a message digest algorithm using cryptography to detect sinkhole attacks [27]. In this system the sinkhole node is detected using an authentication key. When a node advertises new path information the node receiving it creates a digest of the message and sends it both via the original path and the path containing the suspect node. If the new node compromises the message the digest will be incorrect. The receiving node will then detect the compromised node [27]. This approach has two problems. The first is the assumption that the intruder will immediately begin altering messages rather than waiting until it is firmly established in the network or receives instructions to do so. The second is the overhead of calculating the message digest and transmitting messages twice.

Papadimitriou *et al.*, proposed two protocols, RESIST-0 and RESIST-1, that use a cryptographic approach in routing protocols to address the problem of sinkhole attacks [28, 29]. In their approach messages from the base station are verified by the node after obtaining a public key. All authentication activity and signing of data message are done using public and private keys pre-established before the network is deployed. RESIST-1 prevents malicious nodes from lying about their advertised distance to base station more than one hop while the more complex RESIST-0 prevents any lying about advertised distances. The behaviors of malicious nodes of forging packets and hiding their ID's are prevented by this technique. This proposed solution focuses on resistance to sinkhole attacks rather than detection and elimination. The authors argue that the costs in memory and CPU usage of these protocols is manageable [29]

4. 4. Hybrid Approaches

A Hybrid Intrusion detection system was proposed by Coppolino and Spagnuolo to detect sinkhole and sleep deprivation attacks [17]. The proposed system combines anomaly and signature-based detection. The Hybrid Intrusion detection system shares the resources of the sensor nodes. Detection of anomalous behavior used to insert suspicious nodes on a blacklist after analyzing data collected from neighbors. Then the central agent makes a final decision based on features of the attack pattern (misused based) after receiving the blacklist. However this solution was designed for static wireless sensor networks [17].

A radio signal strength based method is proposed by [30], where each node is assigned a unique ID including its location as determined using GPS. When messages are exchanged within the network this unique ID is included and the message is made tamper-resistant. Each node monitors two values, expected signal strength and actual

signal strength. If the difference between the two is greater than some prescribed threshold value the node is treated as suspicious.

5. Conclusion

The application domain in which a wireless sensor network is deployed must determine the level of security required. In our opinion, security in wireless sensor networks is mandatory due to vulnerabilities resulting from the network being unattended resulting in a large number of potential security issues that can be traced back to the leaf sensors. At the same time, the predicament of WSN constraints limits the approaches to security that can be employed. From the study conducted above, we recommend that the system architects will have to decide on the level of security required and value of data turned in for processing. The computational resources required to send individual packets from one node to another, amplified on stochastic model of the whole network signaling will give more accurate picture of the resources drained in signaling. Security measures such as two way verification, encryption, or aggregation will cost resources on top of signaling. If the network architect could map the data value over the consumption of resources for security, it might give better outlook on decision making.

6. Future Research

We aim at designing a secure node to node multichip sensor platform for surveillance and monitoring of industrial equipment. The autonomous sensors and robots should make a robust and self-configuring environment due to somewhat hostile and costly maintenance facets. The sensors are deployed for environmental monitoring and scenario-based surveillance of the area. In this situation, an adversary can inject customized code into the bootstrap of the sensor nodes and hijack the node altogether. In absence of valuable information scaled from the compromised node, the effect on automatic decision making could be markedly different. In the same network, multi sourced temperature information is, on the other hand, not very valuable information hence the need to implement security measures on signaling could prove to be not cost effective. We aim to customize tinyOS and Aurdino nodes for customized network and scenario development.

References

[1] C. Rong, S. Eggen and H. Cheng, “A novel intrusion detection algorithm for wireless sensor networks”, 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), **(2011)**, pp. 1-7.

[2] C. Chen, M. Song and G. Hsieh, “Intrusion detection of sinkhole attacks in large-scale wireless sensor networks”, 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, **(2010)**, pp. 711-716.

[3] L. Teng and Y. Zhang, “SeRA: A Secure Routing Algorithm Against Sinkhole Attacks for Mobile Wireless Sensor Networks”, 2010 Second International Conference on Computer Modeling and Simulation, **(2010)**, pp. 79-82.

[4] K. Sharma and M. Ghose, “Wireless sensor networks: An overview on its security threats”, Int. J. Comput. Their Appl., **(2010)**, pp. 42-45.

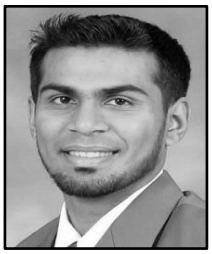
[5] E. C. H. Ngai, J. Liu and M. Lyu, “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks”, 2006 IEEE International Conference on Communications, **(2006)**, pp. 3383-3389.

[6] D. Martins and H. Guyennet, “Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey”, 2010 13th International Conference on Network-Based Information Systems, **(2010)**, pp. 313-320.

[7] P. Samundiswary, D. Sathian and P. Dananjayan, "Secured Greedy Perimeter Stateless Routing For Wireless Sensor Networks", Int. J. Ad hoc, Sens. Ubiquitous Comput., vol. 1, no. 2, **(2010)** June, pp. 9-20.
[8] A.-S. K. Pathan, Ed., "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET", Hoboken, NJ, USA: Taylor and Francis, **(2010)**.
[9] K. Sharma, M. Ghose and D. Kumar, "A comparative study of various security approaches used in wireless sensor networks", Int. J. Adv. Sci. Technol., vol. 17, **(2010)**, pp. 31-44.
[10] A. Pandey and R. C. Tripathi, "A Survey on Wireless Sensor Networks Security", Int. J. Comput. Appl. IJCA, vol. 3, no. 2, **(2010)** October, pp. 43-49.
[11] E. C. H. Ngai, J. Liu and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks", Comput. Commun., vol. 30, no. 11-12, **(2007)** September, pp. 2353-2364.
[12] S. D. Roy, S. A. Singh, S. Choudhury and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management", 2008 IEEE Symposium on Computers and Communications, **(2008)**, pp. 537-542.
[13] J. Sen, "A Survey on Wireless Sensor Network Security", Int. J. Commun. Networks, vol. 1, no. 2, **(2009)**, pp. 59-82.
[14] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks", WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, vol. 3, **(2005)**, pp. 253-259.
[15] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting Sinkhole attacks in wireless sensor networks", ICROS-SICE International Joint Conference, **(2009)**, pp. 1966-1971.
[16] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), **(2009)**, pp. 1-5.
[17] L. Coppolino, S. D'Antonio, L. Romano and G. Spagnuolo, "An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies", 2010 5th International Conference on Critical Infrastructure (CRIS), **(2010)**, pp. 1-8.
[18] I. Krontiris, T. Dimitriou, T. Giannetsos and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks", ALGOSENSORS'07 Proceedings of the 3rd international conference on Algorithmic aspects of wireless sensor networks, **(2007)**, pp. 150-161.
[19] I. Krontiris, T. Giannetsos and T. Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side", 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, **(2008)**, pp. 526-531.
[20] G. H. Raghunandan and B. N. Lakshmi, "A comparative analysis of routing techniques for Wireless Sensor Networks", 2011 National Conference on Innovations in Emerging Technology, **(2011)**, pp. 17–22.
[21] D. Sheela, C. N. Kumar and G. Mahadevan, "A non cryptographic method of sink hole attack detection in wireless sensor networks", 2011 International Conference on Recent Trends in Information Technology (ICRTIT), **(2011)**, pp. 527-532.
[22] M. Mathews, M. Song, S. Shetty and R. McKenzie, "Detecting Compromised Nodes in Wireless Sensor Networks", Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), vol. 1, **(2007)**, pp. 273-278.
[23] H. Song, L. Xie, S. Zhu and G. Cao, "Sensor node compromise detectionn: The Location Perspective", Proceedings of the 2007 international conference on Wireless communications and mobile computing - IWCMC '07, **(2007)**, pp. 242.
[24] Q. Zhang, T. Yu and P. Ning, "A Framework for Identifying Compromised Nodes in Sensor Networks", 2006 Securecomm and Workshops, **(2006)**, pp. 1-10.
[25] J. Xu, J. Wang, S. Xie, W. Chen and J. Kim, "Study on intrusion detection policy for wireless sensor networks", Int. J ournal Secur. Its Appl., vol. 7, no. 2, **(2013)**, pp. 1-6.
[26] D. Dallas, C. Leckie and K. Ramamohanarao, "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks", 15th IEEE International Conference on Networks, **(2007)**, pp. 176-181.
[27] S. Sharmila and G. Umamaheswari, "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms", 2011 International Conference on Process Automation, Control and Computing, **(2011)**, pp. 1-6.
[28] A. Papadimitriou, F. Le Fessant, A. C. Viana and C. Sengul, "Cryptographic protocols to fight sinkhole attacks on tree-based routing in Wireless Sensor Networks", 2009 5th IEEE Workshop on Secure Network Protocols, **(2009)**, pp. 43-48.
[29] F. Le Fessant, A. Papadimitriou, A. C. Viana, C. Sengul and E. Palomar, "A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis," Comput. Commun., vol. 35, no. 2, **(2012)** January, pp. 234–248.

[30] W. R. Pires Junior, T. H. de P. Figueiredo, H. C. Wong and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks", 18th International Parallel and Distributed Processing Symposium, 2004. Proceedings, **(2004)**, pp. 24–30.

Authors



Dr. Junaid Chaudhry specializes in Research and Analysis (R&A) of both network and application centric products. He received his PhD from Ajou University.

He is affiliated with Chonbuk National University and owns an Information Security consultancy, Duja Inc. in Australia that provides tactical consultancy about security solutions of diverse types and development of tailored secure solutions.

Usman Tariq is Computer Scientist and faculty at SAU. He received his MS and PhD from Ajou University. His research interests span networking and security fields. His current research is focused on several network security problems: botnets, denial-of-service attacks, and IP spoofing.

Mohammed Arif Amin received his Bachelor's degree in Electronics Engineering from Near East University, North Cyprus in 1994. He received his Master in Information, Networks and Computer Security from New York Institute of Technology, USA in 2007 and PhD in Computer Science from Universiti Technologi Malaysia in 2012. He is currently a senior lecturer at the department of Computer and Information Science at Higher Colleges of Technology; U. A. E. His research interests are mobility, security in wireless networks and cloud computing.

Dr. Robert G. Rittenhouse is an associate professor at Keimyung Adams College in Daegu Korea. He received his Ph.D. from the University of California at Irvine in 1987. His research interests include security, ubiquitous computing and social informatics

