INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 4064 Cities in 176 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Education/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the authors have seen and agreed to the submitted version of the manuscript and their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
WhatsApp or Viber is active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.
g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, funding institutions, etc., if any.

5. **ABSTRACT**: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

6. **JEL CODE**: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at **www.aeaweb.org/econlit/jelCodes.php**

7. **KEYWORDS**: JEL Code must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

8. **MANUSCRIPT**: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. *It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited*.

9. **HEADINGS**: All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS**: All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**: The main text should follow the following sequence:

INTRODUCTION
REVIEW OF LITERATURE
NEED/IMPORTANCE OF THE STUDY
STATEMENT OF THE PROBLEM
OBJECTIVES
HYPOTHESES
RESEARCH METHODOLOGY
RESULTS & DISCUSSION
FINDINGS
RECOMMENDATIONS/SUGGESTIONS
CONCLUSIONS
LIMITATIONS
SCOPE FOR FURTHER RESEARCH
REFERENCES
APPENDIX/ANNEXURE
It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

12. **FIGURES & TABLES**: These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

13. **EQUATIONS/FORMULAE**: These should be consecutively numbered in parentheses, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilized. If any other equation editor is utilized, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that do not have the editor.

14. **ACRONYMS**: These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES**: The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. Also check to make sure that everything that you are including in the reference section is cited in the paper. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- Headers, footers, endnotes and footnotes may not be used in the document, but in short succinct notes making a specific point, may be placed in number orders following the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

A LITERATURE REVIEW OF TECHNIQUES OF CONCEALING SINK NODES IN WIRELESS SENSOR NETWORKS

RASMEET KAUR
STUDENT
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
GURU NANAK DEV UNIVERSITY
AMRITSAR

KIRANBIR KAUR
ASST. PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
GURU NANAK DEV UNIVERSITY
AMRITSAR

ABSTRACT

Wireless Sensor Networks (WSNs) have been used in a variety of applications to observe various objects. The location security of the Base Station is becoming one of the major issues in WSN due to its critical placement. The issue requires great protection. The privacy of the message can be protected through encryption content. This paper formalizes a novel efficient privacy preserving scheme to secure sink node location. The aim is to keep the location security of the base station from being located by using the traffic flow passive analysis. F-CSH is based on the hiding of the location of the main sink using fake sink holes been elected using fuzzy score function. Also, evaluations prove that the F-CSH technique greatly reduces both the delivery time and conservation energy cost as compared to existing strategies. The overall motive of this paper is to make a comparison of the various secured sink based techniques. At the end of the paper, suitable future directions to enhance this work further are provided.

KEYWORDS
F-CSH, multiple path segments, sink privacy.

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a network composed of resource-constrained devices having limited capabilities, and are called the sensors. The sensors are equipped with wireless communications facilities. These sensors send data to the main node in the Wireless Sensor Network (WSN) which is called the Base Station (BS). The Wireless Sensor Networks (WSNs) are deployed in a variety of applications. The applications of Wireless Sensor Networks (WSNs) vary from homeland security to environment sensing, health monitoring, forest fire detection, manufacturing tasks and many more applications.

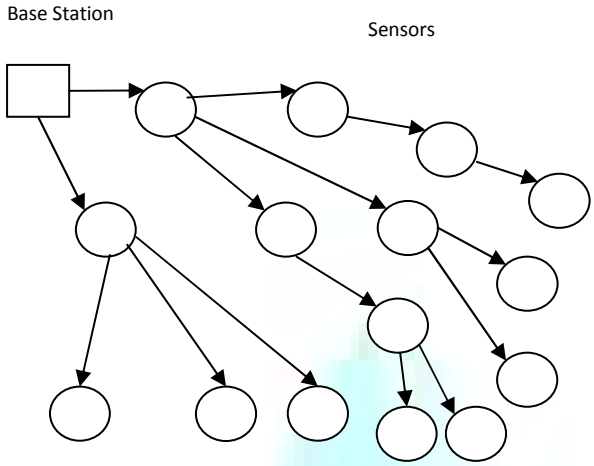
The messages in the Wireless Sensor Network (WSN) are subject to many of the vulnerabilities. The messages may be eavesdropped from the channel and fake messages may be injected into the network without the need of physical access to the network components. The Wireless Sensor Network (WSN) is subject to eavesdropping at the nodes level too. If an opponent gets full access over a node, he may steal the important information from the node, or may change the programming of the node and hence change its behavior, or may physically damage the hardware. In addition, the topology needs to be kept care of. A Wireless Sensor Network (WSN) needs to be secure for its proper functioning. The main features of a secure Wireless Sensor Network (WSN) are the availability, integrity, confidentiality, privacy, authorization, and authentication. A WSN needs to possess these features to work as a secure WSN.

The security of a Wireless Sensor Network (WSN) is challenged by many of the attacks to the WSN. The attacks in the Wireless Sensor Network can be categorized into many of the categories depending upon their intent and the effect. The attacker is an insider or an outsider; the attacks are active or passive; what is the actual purpose of attack, are the main considerations for the categorization of the attacks. Many of the attacks in the wireless sensor network can be categorized as Active Attacks, Passive Attacks, Flood Attacks, Black hole Attack, Denial of service Attack (DoS), Sybil Attack, Information Alteration, Worm Holes, Looping, and Node Replication.

- **Active Attacks** are the attacks in which the attacker causes physical damage in the network like destruction of resources, change of data, changing traffic direction or restriction of data to sink nodes.
- **Passive Attacks** are another types of attacks in which the attackers only observe various activities on the network, extract private information but don't cause any physical destruction or any change of information. Passive attackers can launch active attacks.
- In **Flood Attacks**, Hello messages are flooded in the network. The attacker pretended that the sender of the packet is in their neighbor, therefore when the sender node want to send any sensed information to a sink node, then they forward it towards the attacker node.
- In **Black Hole Attacks**, the attacker nodes act like a black hole, where the attacker node sees the route request packets from its neighbors and replies them back using fake information about shortest route toward sink node. Therefore, any node which wants to send data to a base station will forward it towards attacker.
- In **Denial of Service (DoS) attack**, the attacker sends extra packets in the network without any need and keeps the route as well as the base station busy. So the legitimate users are unable to send data, access resources and get services.
- In **Sybil Attacks**, a node changes its ID continuously and attacker nodes using multiple identities of the legitimate sensor nodes at the same time.
- In the **Information Alteration Attack**, an attacker may spool the data in the middle of communication, and he may alter the complete message or a part of it to misguide the base station.
- In the **Worm Holes Attack**, the whole traffic of the network is sent in a particular direction at a distant place, which causes restriction of data receiving in the other parts of the network.
- In **looping attack**, few nodes in the network cause the circulation of data in a restricted region which stops the data to send to the destination node.
- In the **Node Replication Attack**, the attacker adds a new sensor node in the network, which is using the ID of a trusted user and can attack any node or sink node by pretending himself as a trusted user.

F-CSH is a fuzzy based scheme for concealing sink node with fake holes. The scheme uses the traffic flow passive analysis for concealing sink node. The algorithm works in three phases. The three phases are Network Discovery Phase, Fake Sink Holes Announcement Phase and, Data Delivery Paths Phase. In the Network Discovery Phase, the sink node broadcasts the identification message holding the id. Each node estimates how far it is from the sink node using the RSSI (Received Signal Strength Indication) of this message. Each node broadcasts this message to every other node. During the Fake Sink Holes Announcement Phase, nodes calculate their fuzzy score based on the residual energy of the node, connectivity factor and the centrality factor of the node. The nodes with the highest fuzzy function are selected as the fake sink holes of the current round. In the Data Delivery Phase, nodes send multi-casted packet holding the address of its fake sink hole and randomly one of the nearest neighbors to the target real sink node. This method is repeated by the intermediate nodes on the path from the source node to the real sink.

FIG. A: WIRELESS SENSOR NETWORK



2. LITERATURE SURVEY

Since the location privacy of the sink node is an important issue in wireless sensor networks (WSNs), it requires great protection. A. Din et al. [1] proposed an original and capable privacy protecting method to protect the sink node location. The scheme keeps the location privacy of the sink node from being known. The method uses the traffic flow passive analysis. The method elects fake sink holes for concealing the location of the main sink. The election of the fake sink holes is based on the fuzzy logic.

Black hole attack occurs when a mediator investigates and re-programs some of the nodes in the network. The mediator blocks/drops the packets and generates false messages towards the base station. B. Mishra et al. [2] studied the techniques proposed for the identification and prevention of black hole attack in wireless sensor network. These identify the black hole attack and provide the successful delivery of data to the base station. It is observed that the techniques suffer from very little false positives. A number of security algorithms like AES, DES, XXTEA have been proposed to deal with the black hole attack. The features of each of the algorithms has been studied and compared.

R. Banerjee et al. [3] proposed a new scheme for optimal energy utilization. The scheme is based on cluster based routing protocol. The sink node is considered to be mobile. The cluster head is selected by using the fuzzy function. Agent node selection algorithm is also used for selecting cluster head and Agent node. In addition to the node's energy, the node's distance to Base Station and node's distance to other members is also considered while calculation the fuzzy score. The new protocol is compared with the traditional LEACH protocol. The Simulation results show that the network lifetime improves by an average of 50% in comparison to the traditional LEACH protocol.

Black Hole presents a shortest path to the destination node but in reality it drops all packets. So, security is threatened. G. Pathak et al. [4] proposed a new protocol to protect against the Black Hole attack in Wireless Sensor Networks (WSNs). The protocol uses the Hierarchical Cluster Topology. The proposed protocol has been compared with one of the existing approach in terms of packet delivery ratio, throughput and end-to-end delay using Network Simulator Tool NS2. The new protocol is robust against both single and cooperative Black Hole attacks in a dynamic environment.

In a sinkhole attack, an attacker compromises a node or introduces a fake node inside the network and uses it to commence an attack. J. Chaudhry et al. [5] described the problems in investigating sinkhole attacks in WSNs. Many approaches such as the anomaly-based, rule-based, statistical, cryptographic and hybrid approaches are available for the sinkhole attack detection and prevention. The choice of the approach depends on the particulars of the WSN in question. For example, WSNs where new nodes are not added after initial setup are suited for a rule based approach. A WSN where the sensor nodes are difficult to challenge and have sufficient power are suited for a cryptographic approach.

In a WSN, a large number of sensor nodes are identified to spread out in a geometric region, with close by nodes communicating with each other directly. W. Wei et al. [6] studied the topology discovery with boundary recognition in a wireless sensor network. The scheme detects the holes in the topological architecture of sensor nets only by connectivity information. PPA (Poincare-Perelman Theorem) has been designed to decide whether there are holes in WSNs-monitored areas. The theorem can detect holes on the topological surfaces. These surfaces can, then, connect into meaningful boundary cycles. The method has been proved to be suitable for continuous geometric domains as well as for discrete domains. The algorithm even gives good results in networks with low density.

Coverage holes have become an important problem in Wireless Sensor Networks (WSNs). Coverage is an important pointer to measure if the wireless sensor networks' performance is good or bad. J. Yang et al. [7] proposed two algorithms based on the traditional VOR algorithm to develop the coverage holes recovery. The simulation results establish that these algorithms make holes recovery more effective than the traditional algorithm. The proposed algorithms are the VORP and VORCP algorithm. The results show the betterment of the proposed algorithms in terms of both performance and efficiency.

A wide variety of attacks are known that the wireless sensor networks could suffer. The attacks affect the power consumption and performance of these networks. P. Sanchez et al. [8] simulated the most familiar and dangerous attacks that a WSN can experience. NS-2 and OMNET++ are the simulators that have been used to model WSNs. The simulation technique used is the native HW/SW Co-Simulation. The proposed virtual platform includes a HW node, embedded SW, a RTOS, a wireless sensor network and attack models. The simulations show that three types of attacker nodes have been identified: link-noise, fake-packet injection and direct attack nodes. The affect of these attacks on power utilization and software execution time are also studied. The results show that the given technique is able to investigate the functional and power utilization impact of attack on WSNs.

Security is of major concern in Wireless Sensor Networks (WSNs). M. Khan et al. [9] identifies different challenges and necessities for security of wireless sensor networks. A number of security methods for wireless sensor networks had been proposed. The weaknesses of existing methods have been identified. Different security threats and possible attacks have been analyzed. Different security protocols like the SNEP protocol, TESLA with Instant Key Disclosure (TIK), REWARD have been discussed. The existing security approaches proposed by different researches with their basic characteristics have also been analyzed. However attack identification and prevention has been abandoned.

L. Feng et al. [10] proposes a multi-path energy hole avoidance routing algorithm based on genetic algorithm (GA). The algorithm uses the Genetic Algorithm to select numbers of next-hop nodes and allocate suitable magnitude of data to be transmitted. The proposed algorithm redefines the code, operations and policies of searching optimal solution for the genetic algorithm. The algorithm can not only be applicable to flat networks. It would also be applicable to hierarchical networks, if improved. The algorithm can provide global optimal routing approach for energy balance without assuming the topology structure of network. The simulated experiments show the accuracy of the algorithm. But, there is deficiency of centre optimization device.

Since energy is a limited resource in Wireless Sensor Networks (WSNs), techniques need to be developed which save energy. One such technique is data aggregation. Data aggregation is a collection of data readings that represents a joint view of a set of nodes. Although data aggregation reduces collisions due to

interference and eliminates redundancy, it makes data integrity verification more complex since the received data is distinctive. Bagaa et al. [11] presented a new protocol called SEDAN (Secure and Efficient Data Aggregation protocol for wireless sensor Networks) that provides control integrity for aggregation in wireless sensor networks. It is based on a two-hop verification mechanism of data integrity. It allows us to avoid referring to the base station for data integrity verification. Therefore, SEDAN minimizes the blind rejection of sensed data. In addition, SEDAN saves many useless transmissions between sensors and the sink, and thus minimizes energy consumption. Simulations and comparisons of different techniques and SEDAN using the TinyOS environment show that SEDAN saves energy and minimizes blind rejection while providing the same level of security for aggregated data. In addition, the mean time to bogus data detection (MTTD) in SEDAN is less than in other techniques.

Contextual information such as the information regarding whether, when, and where the data is collected cannot be protected using only native techniques (e.g., encryption). Contextual information can be protected against global eavesdropper who can monitor the entire network traffic by periodic packet transmission combined with dummy traffic filtering at proxy nodes. Bicakci et al. [12] used a Linear Programming (LP) framework to characterize the network dynamics and energy dissipation trends. PFS (Proxy based Filtering Scheme) and TFS (Tree based Filtering Scheme) schemes proposed earlier have been modeled. PFS scheme uses a single level proxy architecture, where data packets pass through a single proxy at most. Both ordinary nodes and proxy nodes always generate data at a steady rate. In TFS scheme, proxies are organized in a tree structure; proxies at higher levels in the tree aggregate the packets coming from lower level proxies. Bicakci et al. proposed and modeled a new scheme called OFS (Optimal Filtering Scheme). PFS is suitable for small-size WSNs. As network size grows, the OFS becomes more significant for use than the PFS.

Data trustworthiness is a fundamental requirement in a Wireless Sensor Network (WSN). Location-aware sensors are becoming the reality standard in WSNs. The trustworthiness about the node position information and the privacy conformity are used for evaluating data trustworthiness. Trustworthiness, security of localization information and privacy are the fundamental requirements in WSN. Porisini et al. [13] presented an approach, named Cross Layer Protocol (CLP), for improving data quality based on an integrated solution that considers a sound privacy management policy along with a secure localization protocol. The approach is largely independent from the adopted routing protocols, the verification localization algorithm and the used encryption technique. CLP relies on cross-layer evaluation to assess the overall quality of the collected information. CLP combines verification of localization information and the identification of privacy violations and, thus, evaluates nodes reputation and therefore data quality. The simulations were carried out using Omnet++. The obtained results from the simulations prove that besides guaranteeing anonymity, CLP provides secure node localization and the capability to identify malicious behaviors.

Two-tier architecture has been widely adopted for Wireless Sensor Networks (WSNs) because it can save power and storage consumptions for sensors and improve the efficiency of query processing. In a two-tiered wireless sensor network, resource-constrained sensor nodes act as the lower layer and sense data, and resource-rich storage nodes act as the upper layer and store data and process queries from the sink. But, the storage nodes may be attacked in an unfriendly environment and violate privacy of sensor data. Yao et al. [14] proposed a privacy-preserving protocol specializing for MAX/MIN query that prevents eavesdroppers from gaining sensitive information from sensor collected data.

One way of hiding the sensor nodes' detectability is by limiting the transmission power of the nodes that eavesdroppers cannot detect the existence of the WSN unless they are within the sensing range of the WSN. The network is said to be operating in the stealth mode. Position dependent transmission power adjustment enables the network to maintain its level of secrecy while allowing nodes farther from the network boundary to use higher transmission energy levels. In order to mitigate the irregular energy dissipation characteristic, nodes that cannot disperse their energies on communications reduce the amount of data they generate through computation so that the relay nodes convey less data. Compression/decompression techniques can be used to reduce the amount of data generated. Dynamic data compression/decompression strategies achieve better energy savings when compared to static compression/decompression of data in which the data is always compressed independently of the power transmission strategy. Incebacak et al. [15] employed contextual privacy measures through a novel mathematical programming framework. Five data compression strategies are employed which are No Compression (NC) strategy, Always Compression (AC) strategy, Optimal Compression (OC), Optimal Single Level Compression (OSLC), and Limited Compression (LC). Inceback et al. [15] also investigated the effects of Optimal Single Level Compression (OSLC) and Limited Compression (LC) strategies through Mixed Integer Programming (MIP) models. The impact of node density and limited transmission range due to contextual privacy scenarios are explored.

Several privacy-preserving techniques for Wireless Sensor Networks (WSNs) are available. There are two main categories of privacy-preserving procedures for protecting two types of private information, data-oriented and context-oriented privacy. First is privacy concern on information being collected, transmitted, and analyzed in a Wireless Sensor Network (WSN) and that of sensitive queries executed. Second is the protection of contextual information such as the location of a sensor initiating data communication and the base station as well as the timing of the generation and transmission of sensitive data. Effective countermeasure against the disclosure of both data and context-oriented private information is an indispensable prerequisite for the broad application of WSNs to real-world applications. Li et al. [16] provided a state-of-the-art survey of privacy-preserving techniques for WSNs. Privacy protection has been extensively studied in various fields related to WSN such as wired and wireless networking, databases and data mining. Li et al. attempted to compare the existing techniques in terms of such metrics as privacy, accuracy, delay, and power consumption. A number of important open challenges are discussed for future research.

Securing surveillance wireless sensor networks (WSNs) during Base Station (BS) failure is challenging. BS is a critical part of a WSN and the whole WSN can be made useless by taking down its BS. The eavesdroppers can make the network useless by only destroying the BS as the required efforts to destroy the BS is much less than that is needed to destroy the network. Megahed et al. [17] proposed a novel security architecture called Surveillance Security (SurvSec) for efficient network recovery from single BS failure of surveillance WSN with single BS. The new designed security architecture will detect the BS failure, monitor the network sensitive security issues to store security data in multiple replicas, and send the stored data to the new Base Station after it is authenticated. SurvSec employs a set of sensor nodes to work as Security Managers for management and storage of the security concerned data of all sensor nodes. SurvSec has three components: (1) Sensor nodes serve as Security Managers, (2) Data Storage System, and (3) Data Recovery System. Megahed et al. evaluated the designed security architecture for reliable network recovery from BS failure. The evaluation showed that the proposed security architecture can meet all the desired specifications and the provided Security Managers are capable of network recovery from BS failure.

Concealing the locations and the identities of the nodes, especially the sink node or the Base Station in a wireless sensor network (WSN) is challenging. Nezhad et al. [18] explained that appropriate solutions for this problem depend on the nature of the traffic generated in the network and the capabilities of the eavesdropper that must be resisted. Nezhad et al. proposed a DCARPS anonymous routing protocol that can support location privacy against a global eavesdropper. The protocol is based on label switching. Layered cryptography has been used to make a packet look randomly different on consecutive links. To have energy conservation, the Destination-Controlled Anonymous Routing Protocol for Sensornets (DCARPS) for abundant traffic situations use only modest symmetric cryptography. In addition, the sink is responsible for all routing calculations while the sensors only perform simple label swapping actions when forwarding packets. Another advantage of labels is preventing unnecessary cryptographic operations. DCARPS is suitable for abundant traffic networks but two variations of this protocol called Probabilistic DCARPS are also available for scarce traffic networks.

Pietro et al. [19] addressed the problem of preserving the location privacy of the sensors of a wireless sensor network when they send reply to a query broadcast by the Base Station. These queries focus on obtaining aggregate features such as SUM, AVERAGE, or MAX/MIN of data readings. These values are provided by the sensors to the sink. Therefore, preserving location privacy is an important aspect in such situations. In addition, resilience is another important feature to be met which assures that assures that the overall computation is not disturbed by a subset of sensors compromised by eavesdropper. A probabilistic and scalable protocol is provided in the paper. The protocol has the following features: (i) it ensures the location privacy of the sensors replying to the query (ii) it is resilient to an active eavesdropper willing to change the readings sent by the sensors; and, (iii) it allows to trade-off the accuracy of the result with (a small) overhead increase [19].The protocol ensures that even an adversary that can monitor the whole network, it cannot extract any information about the sensors that have the value queried by the Base Station. The protocol is lightweight and expandable; communication overhead is evenly distributed among sensors.

End-to-end data integrity is an important concern in Wireless Sensor Networks (WSNs). Whenever the number of messages in the transmission buffer increases than a given threshold, messages are aggregated to eliminate the buffer overflow. The messages in the transmission buffer are aggregated as soon as the

transmission queue starts increasing in length. Sicari et al. [20] presented an approach for dynamic secure end-to-end data aggregation with privacy function, named DyDAP. It is an innovative and integrated solution for dynamic data aggregation with privacy solution. DyDAP introduces an original aggregation algorithm that uses a discrete-time control loop and is able to dynamically handle data fusion inside the network which reduces the communication load. The protocol has been designed starting from a UML model. Computer simulations have been provided showing that DyDAP avoids network congestion. It improves WSN estimation accuracy; and guarantees anonymity and data integrity.
DyDAP is a building block of several secure Internet of Things (IoT) scenarios.

TABLE 1

Ref No.	Year	Authors	Techniques	Features	Sink Privacy	Source Privacy	Soft Computing	Tools
1	2014	A. Din et al.	F-CSH	Fuzzy logic	Yes	No	Yes	MATLAB
2	2014	A. Mishra et al.	Security against Black Hole Attack	Black hole attack is identified	No	No	No	NA
3	2014	R. Banerjee et al.	Cluster Based Routing Protocol	Energy Hole is by-passed	Yes	No	No	NA
4	2014	G. Pathak et al.	Hierarchical Cluster Topology	Black Hole Attacks are detected and prevented	No	Yes	No	Network Simulator Tool NS2
5	2013	J. Chaudhry et al.	Dealing Sinkhole Attacks	Sinkhole attacks are detected and neutralized	Yes	No	No	NA
6	2012	W. Wei et al.	Poincare-Perelman Theorem	Detects holes by connectivity information	No	No	No	NA
7	2013	J.Yang et al.	VOR, VORP, VORCP algorithm	Coverage holes are detected	No	Yes	No	MATLAB
8	2013	P.Sanchez et al.	Security Simulation	Security and Performance Analysis is perfomed	No	No	No	NA
9	2011	M.Khan et al.	Security Protocols	Security techniques are discussed	Yes	Yes	No	NA
10	2008	L.Feng et al.	Multi-path routing Genetic algorithm	Provides global optimal routing approach	No	Yes	Yes	NA
11	2011	M.Bagaa et al.	Data aggregation	Efficient data aggregation is provided	No	Yes	No	TinyOS
12	2011	K. Bicakci et al.	Life Maximization	Linear Programming (LP) framework is used	No	No	No	NA
13	2012	A. Porisini et al.	Cross Layer Protocol	Data quality is improved	No	No	No	Omnet++
14	2013	Y.Yao et al.	HMAC-MD5 DES algorithm	Two-tier WSN is used	No	No	No	NA
15	2014	D.Incebacak et al.	Optimal Data Compression	Contextual privacy is provided	Yes	Yes	No	NA
16	2009	N.Li et al.	Privacy Preservation	A Survey	Yes	Yes	No	NA
17	2011	M. Megahed et al.	Surveillance Security (SurvSec)	Base Station Failure Recovery is provided	Yes	No	No	Matlab
18	2008	A.Nezhad et al.	DCARPS protocol	Symmetric Cryptography is used	Yes	Yes	No	OPNET
19	2011	R.Pietro et al.	Location Privacy and Resilience	Location Privacy and Resilience	Yes	Yes	No	
20	2012	S. Sicari et al.	DyDAP privacy function	End-to-end data aggregation is provided	Yes	Yes	No	

3. CONCLUSION AND FUTURE WORK

A novel privacy-preserving scheme applying intelligent fake sink node topology to protect the location security of BS has been considered in this paper. In this paper, F-CSL based on the hiding of the main sink using fake sink nodes has been elected using fuzzy score function. The sink location could be replaced with dummy sink nodes. The analysis has evaluated the performance of the new technique and found that the scheme can effectively secure the sink location. The energy utilization and delivery time is also more efficient as compared with others. In near future, I will extended F-CSL further in order to improve sink privacy with multiple path segments using mobility control. My work will also consider the dual membership function to minimize the energy utilization more.

REFERENCES

1. El-Din, Ahmed E., Rabie A. Ramadan, A. A. Elmagid, and Salah A. Aly. "Novel Scheme of Fuzzy based Concealing Sink Node with Fake Holes (F-CSH)."Procedia Computer Science 32 (2014): 1174-1179.
2. Mishra, Binod Kumar, Mohan C. Nikam, and Prashant Lakkadwala. "Security against Black Hole Attack in Wireless Sensor Network-A Review." In Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, pp. 615-620. IEEE, 2014.
3. Banerjee, Ritwik, and Chandan Kr Bhattacharyya. "Energy efficient routing and bypassing energy-hole through mobile sink in WSN." In Computer Communication and Informatics (ICCCI), 2014 International Conference on, pp. 1-6. IEEE, 2014.
4. Pathak, Ganesh R., Suhas H. Patil, and Jyoti S. Tryambake. "Efficient and Trust Based Black Hole Attack Detection and Prevention in WSN."International Journal of Computer Science and Business Informatics 14, no. 2 (2014).
5. Chaudhry, Junaid Ahsenali, Usman Tariq, Mohammed Arif Amin, and Robert G. Rittenhouse. "Dealing with Sinkhole Attacks in Wireless Sensor Networks."Advanced Science and Technology Letters 29 (2013): 7-12.
6. Wei, Wei, Xiao-Lin Yang, Pei-Yi Shen, and Bin Zhou. "Holes detection in anisotropic sensor-nets: Topological methods." International Journal of Distributed Sensor Networks 2012 (2012).
7. Yang, Jianjun, Yuming Mao, Qin Yu, and Supeng Leng. "Researches on coverage holes recovery algorithm in WSN." In Communications, Circuits and Systems (ICCCAS), 2013 International Conference on, vol. 2, pp. 78-83. IEEE, 2013.
8. Díaz, A., P. Sanchez, J. Sancho, and J. Rico. "Wireless sensor network simulation for security and performance analysis." In Proceedings of the Conference on Design, Automation and Test in Europe, pp. 432-435. EDA Consortium, 2013.
9. Khan, Muazzam A., Ghalib A. Shah, and Muhammad Sher. "Challenges for security in wireless sensor networks (WSNs)." World Academy of Science, Engineering and Technology 80 (2011).
10. Liu, An-Feng, Ming Ma, Zhi-gang Chen, and Wei-hua Gui. "A Multi-Path Energy Hole Avoidance Routing Algorithm for WSN Based on GA." In Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on, pp. 1-4. IEEE, 2008.
11. Bagaa, Miloud, Yacine Challal, Abdelraouf Ouadjaout, Noureddine Lasla, and Nadjib Badache. "Efficient data aggregation with in-network integrity control for WSN." Journal of Parallel and Distributed Computing 72, no. 10 (2012): 1157-1170.

12. Bicakci, Kemal, Hakan Gultekin, Bulent Tavli, and Ibrahim Ethem Bagci. "Maximizing lifetime of event-unobservable wireless sensor networks."Computer Standards & Interfaces 33, no. 4 (2011): 401-410.
13. Coen-Porisini, Alberto, and Sabrina Sicari. "Improving data quality using a cross layer protocol in wireless sensor networks." Computer Networks 56, no. 17 (2012): 3655-3665.
14. Yao, Yonglei, Naixue Xiong, Jong Hyuk Park, Li Ma, and Jingfa Liu. "Privacy-preserving max/min query in two-tiered wireless sensor networks." Computers & Mathematics with Applications 65, no. 9 (2013): 1318-1325.
15. Incebacak, Davut, Ruken Zilan, Bulent Tavli, Jose M. Barcelo-Ordinas, and Jorge Garcia-Vidal. "Optimal data compression for lifetime maximization in wireless sensor networks operating in stealth mode." Ad Hoc Networks 24 (2015): 134-147.
16. Li, Na, Nan Zhang, Sajal K. Das, and Bhavani Thuraisingham. "Privacy preservation in wireless sensor networks: A state-of-the-art survey." Ad Hoc Networks 7, no. 8 (2009): 1501-1514.
17. Megahed, Mohamed Helmy, Dimitrios Makrakis, and Bidi Ying. "SurvSec: A New Security Architecture for Reliable Network Recovery from Base Station Failure of Surveillance WSN." Procedia Computer Science 5 (2011): 141-148.
18. Nezhad, Alireza A., Ali Miri, and Dimitris Makrakis. "Location privacy and anonymity preserving routing for wireless sensor networks." Computer Networks 52, no. 18 (2008): 3433-3452.
19. Di Pietro, Roberto, and Alexandre Viejo. "Location privacy and resilience in wireless sensor networks querying." Computer Communications 34, no. 3 (2011): 515-523.
20. Sicari, Sabrina, Luigi Alfredo Grieco, Gennaro Boggia, and Alberto Coen-Porisini. "DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks." Journal of Systems and Software 85, no. 1 (2012): 152-166.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, nor its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal is exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals