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, Polandwith 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 2477 Cities in 159 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

Weinvite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Education, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; 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; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor 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; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

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/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 author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

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:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

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 mentionthe 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.

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. **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.

5. **KEYWORDS:** Abstract 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.

6. **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.

7. **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.

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

9. **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

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **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.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **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**. 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.
- The location of endnotes within the text should be indicated by superscript numbers.

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, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

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

EFFECTIVE DYNAMIC ROUTING PROTOCOL: ANALYSIS OF VARIOUS SECURE DATA ROUTING PROTOCOL AND DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

S.MOHAMED SALEEM
STUDENT
VIT BUSINESS SCHOOL
VIT UNIVERSITY
VELLORE

P.SASI KUMAR
STUDENT
DEPARTMENT OF INFORMATION TECHNOLOGY
SRM UNIVERSITY
KATTANKULATHUR

ABSTRACT

In wireless sensor networks, adversaries can inject false data reports via compromised nodes and launch DoS attacks against legitimate reports. Recently, a number of filtering schemes against false reports have been proposed. However, they either lack strong filtering capacity or cannot support highly dynamic sensor networks very well. Moreover, few of them can deal with DoS attacks simultaneously. In this paper, we propose a dynamic en-route filtering scheme that addresses both false report injection and DoS attacks in wireless sensor networks. In our scheme, each node has a hash chain of authentication keys used to endorse reports; meanwhile, a legitimate report should be authenticated by a certain number of nodes. First, each node disseminates its key to forwarding nodes. Then, after sending reports, the sending nodes disclose their keys, allowing the forwarding nodes to verify their reports. We design the Hill Climbing key dissemination approach that ensures the nodes closer to data sources have stronger filtering capacity. Moreover, we exploit the broadcast property of wireless communication to defeat DoS attacks and adopt multipath routing to deal with the topology changes of sensor networks. Simulation results show that compared to existing solutions, our scheme can drop false reports earlier with a lower memory requirement, especially in highly dynamic sensor networks.

KEYWORDS

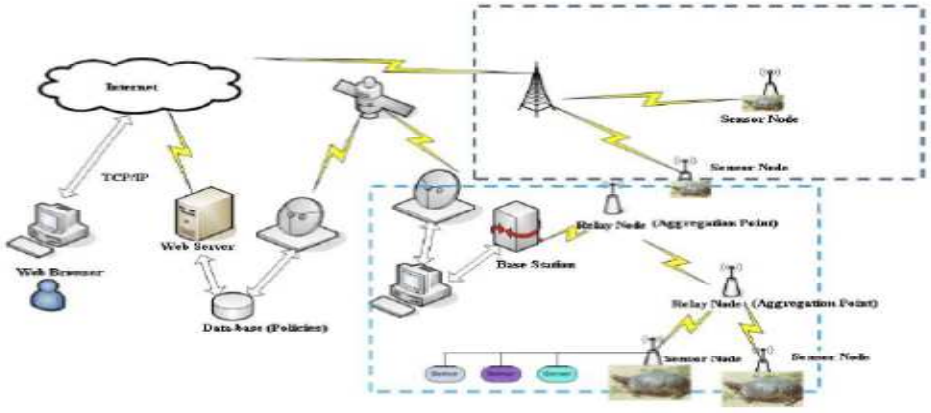
Wireless Sensor Network, Security Routing protocol, Intrusion Detection System (IDS), Data Authenticity and Attacks on sensor network.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are homogeneous or heterogeneous systems consist of many small devices, called sensor nodes, that monitoring different environments in cooperative; i.e. sensor nodes cooperate to each other and compose their local data to reach a global view of the operational environment; they also can operate autonomously. In WSNs there are two other components, called "aggregation points" (i.e. cluster-heads and CIDSs' deployment locations) and "base stations" (i.e. central server and the WSNIDS's deployment location), which have more powerful resources and capabilities than normal sensor nodes. As shown in Figure1, aggregation points collect information from their nearby sensors, integrate and aggregate them and then forward to the base stations to process gathered data. In these large sensor network systems, we need nodes to be able to locate themselves in various environments, and on different distance scales. This problem, which we refer to as localization1, is a challenging one, and yet extremely crucial for many applications of very large networks of devices. For example, localization opens up new ways of reducing power consumed in multi-hop wireless networks. In context-aware applications, localization enables the intelligent selection of appropriate devices, and may support useful coordination among devices. The desired granularity of localization is itself application dependent. GPS solves the problem of localization in outdoor environments for PC class nodes. However, for large networks of very small, cheap and low power devices, practical considerations such as size, form factor, cost and power constraints of the nodes preclude the use of GPS on all nodes.

In this paper, we address the problem of localization for such devices, with the following design goals. RF- based: We focus on small nodes which have some kind of short-range radio frequency (RF) transceiver. Our primary goal is to leverage this radio for localization, thereby eliminating the cost, power and size requirements of a GPS receiver. Receiver based: In order to scale well to large distributed networks, the responsibility for localization must lie with the receiver node that needs to be localized and not with the reference points. Adhoc: In order to ease deployment, we desire a solution that does not require pre-planning, extensive infrastructure. Responsiveness: We need to be able to localize within a fairly low response time .Low Energy: Small, un-tethered nodes have modest processing capabilities, and limited energy resources. If a device uses all of its energy localizing itself, it will have none left to perform its task. Therefore, we desire to minimize computation and message costs to reduce power consumption. Adaptive Fidelity: In addition, we want the accuracy of our localization algorithms to be adaptive to the granularity of available reference points.

FIG.1: WSNS' COMMUNICATION ARCHITECTURE

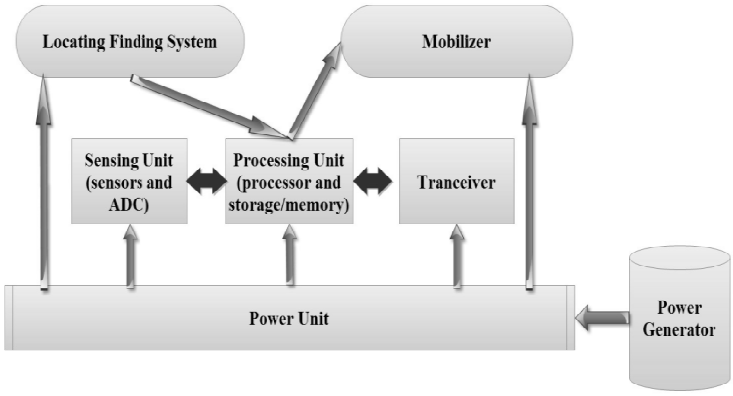


A. WSNs characteristics

A WSN is a homogenous or heterogeneous system consisting of hundreds or thousands of low-cost and low-power tiny sensors to monitor and gather real-time information from deployment environment. Common functionalities of WSNs' nodes are broadcasting and multicasting, routing, forwarding and route maintenance. The sensor's components are: sensor unit, processing unit, memory unit, power supply unit and wireless radio transceiver; these units are communicating to each other, as shown in Figure2. Some of most important characteristics of these networks are:

- Wireless and weak connections
- Low reliability of sensor nodes;
- Dynamic topology and self-organization (unpredictable WSN's topology);
- Ad-hoc based networks and hop-by-hop communications (multi-hop routing);
- Open/hostile nature of deployment environment
- Inter-nodes broadcast-nature communications
- Ease of extendibility (scalability);
- Direct communication, contact and interaction with physical environment

FIG.2: WSN'S NODE ARCHITECTURE



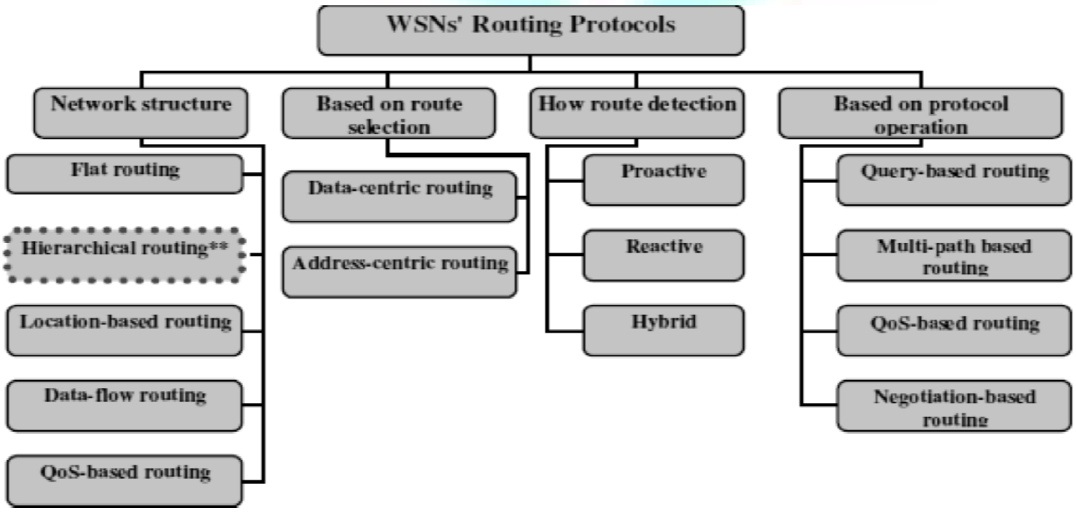
2. ROUTING IN WSNS

A. Effective parameters on designing WSNs' routing protocols

Some of most important desirable criteria in designing WSNs' routing protocols are:

- WSNs' variable and different configurations and dynamic topology
- Different addressing design
- Method of sensor nodes' deployment on the WSN
- Amount of energy consumption/waste
- The most important issue in designing WSNs' different protocols, like routing protocols, is the cost of energy consumption factor. On WSNs, each node usually consumes energy to measure the goal parameter (gather information), transmit and process the raw data. But, the step of data transmission consumes more energy than others.
- Used data transmission and reporting method this is including following models; i.e. time-driven model, event-driven model, query-driven model and combinational model
- Data aggregation In attending to the most energy consumption step of the WSN's processes is data transmission, protocols designers usually try to using data aggregation and processing, compression, compaction and combination techniques to decrease the volume of sent data
- Consistency with operating environment
- Matching with communication channel frequency and transmission media;
- Fairness

FIG.3: ROUTING IN WSN



3. SCHEMES OF LOCALIZATION

Many existing systems and protocols attempt to solve the problem of determining a node's location within its environment. The approaches taken to solve this localization problem differ in the assumptions that they make about their respective network and device capabilities. These include assumptions on device hardware, signal propagation models, timing and energy requirements, network makeup (homogeneous vs. heterogeneous), the nature of the environment (indoor vs. outdoor), node or beacon density, time synchronization of devices, communication costs, error requirements, and device mobility. In

this section, we discuss prior work in localization with regard to these network characteristics, device restrictions, and application requirements. We divide our discussion into two subsections where we present both range-based and range free solutions.

A. RANGE-BASED LOCALIZATION SCHEMES

Time of Arrival (TOA) technology is commonly used as a means of obtaining range information via signal propagation time. The most basic localization system to use TOA techniques is GPS. GPS systems require expensive and energy-consuming electronics to precisely synchronize with a satellite's clock. With hardware limitations and the inherent energy constraints of sensor network devices, GPS and other TOA technology present a costly solution for localization in wireless sensor networks. The Time Difference of Arrival (TDOA) technique for **ranging**(estimating the distance between two communicating nodes) has been widely proposed as a necessary ingredient in localization solutions for wireless sensor networks. While many infrastructure-based systems have been proposed that use TDOA, additional work such as AHLos has employed such technology in infrastructure-free sensor networks.

Like TOA technology, TDOA also relies on extensive hardware that is expensive and energy consuming, making it less suitable for low-power sensor network devices. In addition, TDOA techniques using ultrasound require dense deployment as ultrasound signals usually only propagate 20-30 feet. To augment and complement TDOA and TOA technologies, an Angle of Arrival (AOA) technique has been proposed that allows nodes to estimate and map relative angles between neighbors. Similar to TOA and TDOA, AOA estimates require additional hardware too expensive to be used in large scale sensor networks. Received Signal Strength Indicator (RSSI) technology such as RADAR and Spot On has been proposed for hardware constrained systems. In RSSI techniques, either theoretical or empirical models are used to translate signal strength into distance estimates. For RF systems, problems such as multi-path fading, background interference, and irregular signal propagation characteristic make range estimates inaccurate. Work to mitigate such errors such as robust range estimation, two-phase refinement positioning, and parameter calibration have been proposed to take advantage of averaging, smoothing, and alternate hybrid techniques to reduce error to within some acceptable limit. While solutions based on RSSI have demonstrated efficacy in simulation and in a controlled laboratory environment, the premise that distance can be determined based on signal strength, propagation patterns, and fading models remains questionable, creating a demand for alternate localization solutions that work independent of this assumption.

B. RANGE-FREE LOCALIZATION SCHEMES

In sensor networks and other distributed systems, errors can often be masked through fault tolerance, redundancy, aggregation, or by other means. Depending on the behavior and requirements of protocols using location information, varying granularities of error may be appropriate from system to system. Acknowledging that the cost of hardware required by range-based solutions maybe inappropriate in relation to the required location precision, researchers have sought alternate range-free solutions to the localization problem in sensor networks. In a heterogeneous network containing powerful nodes with established location information is considered. In this work, anchors beacon their position to neighbors that keep an account of all received beacons. Using this proximity information, a simple Centro id model is applied to estimate the listening nodes' location. We refer to this protocol as the Centro id algorithm .An alternate solution, DV-HOP assumes a heterogeneous network consisting of sensing nodes and anchors. Instead of single hop broadcasts, anchors flood their location throughout the network maintaining a running hop-count at each node along the way. Nodes calculate their position based on the received anchor locations, the hop-count from the corresponding anchor and the average-distance per hop; a value obtained through anchor communication. Like DV-Hop, an Amorphous Positioning algorithm proposed in uses offline hop-distance estimations, improving location estimates through neighbor information exchange. These range-free techniques are described in more depth in section 4, and are used in our analysis for comparison with our work.

C. APIT LOCALIZATION SCHEME

In this section, we describe our novel area-based range-free localization scheme, which we call APIT. APIT requires a heterogeneous network of sensing devices where a small percentage of these devices (percentages vary depending on network and node density) are equipped with high-powered transmitters and location information obtained via GPS or some other mechanism. We refer to these location-equipped devices as anchors. Using beacons from these anchors, APIT employs a novel *area-based* approach to perform location estimation by isolating the environment into triangular regions between beaconing nodes (Figure 1). A node's presence inside or outside of these triangular regions allows a node to narrow down the are a in which it can potentially reside. By utilizing combinations of anchor positions, the diameter of the estimated area in which anode resides can be reduced, to provide a good location estimate.

4. SECURITY ISSUES AND GOALS

A. DATA CONFIDENTIALITY

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. Since public-key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods. The creators of tiny Sec argue that cipher block chaining (CBC) is the most appropriate encryption scheme for sensor networks. They found RC5 and Skipjack to be most appropriate for software implementation on embedded microcontrollers. The default block cipher in tiny Sec is Skipjack. SPINS uses RC6 as its cipher.

B. DATA AUTHENTICITY

In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Data authentication prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. In the two- party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. However, authentication for broadcast messages requires stronger trust assumptions on the network nodes. The creators of SPINS contend that if one sender wants to send authentic data to mutually entrusted receivers, using a symmetric MAC is insecure since any one of the receivers know the MAC key, and hence could impersonate the sender and forge messages to other receivers. SPINS constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. LEAP uses a globally shared symmetric key for broadcast messages to the whole group. However, since the group key is shared among all the nodes in the network, an efficient reeking mechanism is defined for updating this key after a compromised node is revoked. This means that LEAP has also defined an efficient mechanism to verify whether a node has been compromised.

C. DATA INTEGRITY

Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Note that Data Authentication can provide Data Integrity also.

D. DATA FRESHNESS

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. A common defense is to include a monotonically increasing counter with every message and reject messages with old counter values. With this policy, every recipient must maintain a table of the last value from every sender it receives Some Researchers contend that protection against the replay of data packets should be provided at the application layer and not by a secure routing protocol as only the application can fully and accurately detect the replay of data packets (as opposed to retransmissions, for example). Whereas some authors reason that by using information about the network's topology and communication patterns, the application and routing layers can properly and efficiently manage a limited amount of memory devoted to replay detection. Mostly Researchers have identified two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful foretime synchronization within the network.

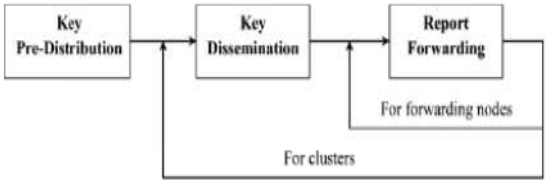
E. **ROBUSTNESS AND SURVIVABILITY**

The sensor network should be robust against various security attacks, and if an attack succeeds, its impact should be minimized. The compromise of a single node should not break the security of the entire network.

5. OVERVIEW OF THE WORK

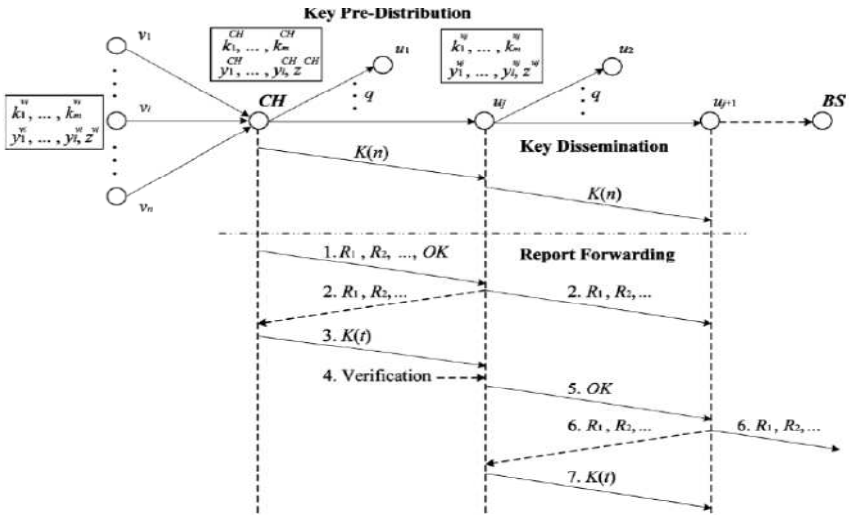
When an event occurs within some cluster, the cluster-head collects the sensing reports from sensing nodes and aggregates them into the aggregated reports. Then, it forwards the aggregated reports to the base station through forwarding nodes. In our scheme, each sensing report contains one MAC that is produced by a sensing node using its authentication key (called auth-key for short), while each aggregated report contains distinct MACs, where is the maximum number of compromised nodes allowed in each cluster. In our scheme, each node possesses a sequence of auth-keys that form a hash chain. Before sending the reports, the cluster-head disseminates the first auth-keys of all nodes to the forwarding nodes that are located on multiple paths from the cluster-head to the base station. The reports are organized into rounds, each containing a fixed number of reports. In every round, each sensing node chooses a new auth-key to authenticate its reports. The processes of verification, overhearing, and key disclosure are repeated by the forwarding nodes at every hop until the reports are dropped or delivered to the base static Specifically, our scheme can be divided into three phases key pre distribution phase, key dissemination phase, and report forwarding phase. In the key pre distribution phase, each node is preloaded with a distinct seed key from which it can generate a hash chain of its auth-keys. In the key dissemination phase, the cluster-head disseminates each node's first auth-key to the forwarding nodes, which will be able to filter false re- ports later. In the report forwarding phase, each forwarding node verifies the reports using the disclosed auth-keys and disseminated ones. If the reports are valid, the forwarding node discloses the auth-keys to its next-hop node after overhearing that node's broadcast. Otherwise, it informs the next-hop node to drop the invalid reports. This process is repeated by every forwarding node until the reports are dropped or delivered to the base station.

FIG.4: THE RELATIONSHIP BETWEEN THREE PHASES OF OUR SCHEME



Key pre distribution is performed before the nodes are deployed, e.g., it can be done offline. Key dissemination happens before the sensing nodes begin to send the reports. It maybe executed periodically depending on how often the topology is changed. Every time the latest (unused) auth-key of sensing nodes will be disseminated. Report forwarding occurs at each forwarding node in every round.

FIG.5: THE DETAILED PROCEDURE OF THREE PHASES



In the key pre distribution phase, each node is preloaded with l+1 secret keys .y1….yn and z, and can generate a hash chain of auth-keys k1…kn from the seed key km. In the key dissemination phase, the cluster-head disseminates the auth-keys of all nodes by message k(n) to q downstream neighbor nodes. Every downstream node decrypts some auth-keys from k(n), and further forwards K(n) to q more downstream neighbor nodes, which then repeat the same operation. In the report forwarding phase, each forwarding node en-route performs the following steps: 1) It receives the reports from its upstream node. 2) If it receives confirmation message OK then forwards the reports to its next-hop node. Otherwise, it discards the reports. 3) It receives the disclosed auth-keys within message k(t)and verifies the reports by using the disclosed keys. 4) It informs its next-hop node the verification result.

6. THE PROPOSED INTRUSION DETECTION ARCHITECTURE (IDA) FOR WIRELESS SENSOR NETWORKS

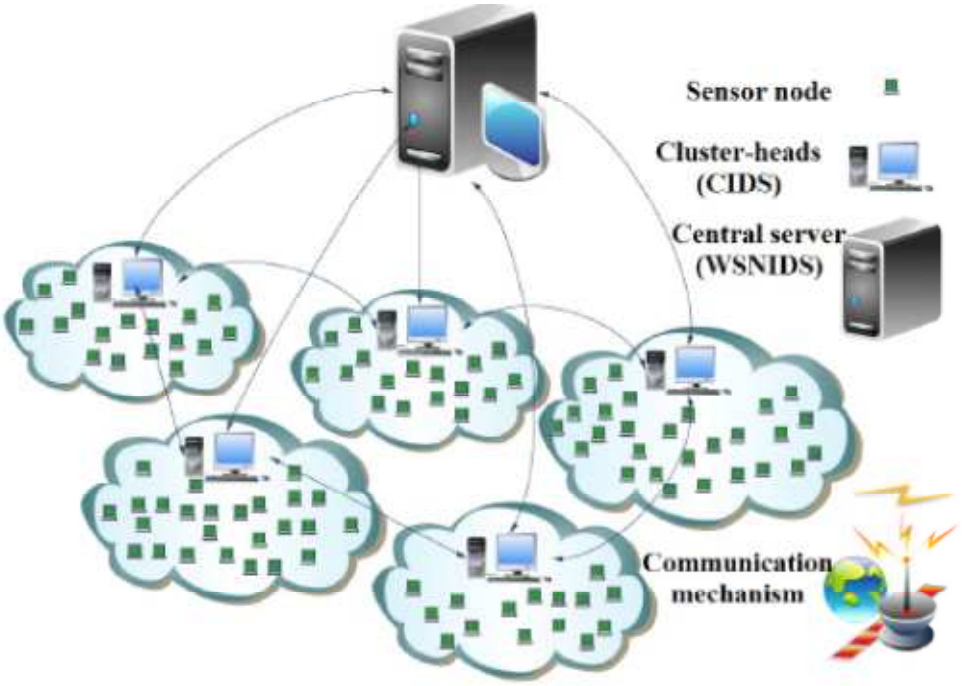
As Figure6 is showing, the suggestion architecture has a combinational (distributed and centralized) and hierarchical structure; thus, the proposed approach can be used in 1 or 2 levels of IDSs:

A. Cluster-based Intrusion Detection System (CIDS)

CIDSs place on the low level of the proposed architecture (according to the Figure6); i.e. they install and deploy on the heterogeneous cluster-heads. There is a cluster-head per each cluster of sensor nodes which it covers its radio range nodes; so, the intrusion detection process does by cluster-heads. There is a small and low-size policy-base (Cluster-Based Policy Base: CBPB) on each cluster-head that includes the most common patterns of attacks on this domain, along with special and limited preprocessing capabilities such as requirement data field extraction from the network packets and packets filtering. If an attack detects, according to the predefined action in policy and corresponding security rule, the IDS is responding to it. In this level, decision making does in combinational; so, if the current traffic be from the internal of the cluster, the appropriate decision takes autonomously and independently; also, if the current traffic be from the

boundary nodes (between different adjacent clusters), the collector be selected and then, the collector enforces the majority rule to takes the final decision; finally, if the current traffic not be about an intrusion or the collector can not take a decision (if the majority rule be inefficient), for more consideration, that traffic labeled (for example, rely on the attack estimation severity by current node) and will forward to the central server (centralized-cooperative decision making by CIDSs and WSNIDS).

FIG.6: THE PROPOSED INTRUSION DETECTION ARCHITECTURE (IDA) FOR WSNS



7. SIMULATION RESULTS

In summary, simulation results show that our scheme has the following advantages when compared with others:

1)Our scheme drops false reports earlier even with a lower memory requirement. In some scenario, it can drop false reports in 6 hops with only 25 keys stored in each node, but another scheme needs 12 hops even with 50 keys stored.

2) Our scheme can better deal with the dynamic topology of sensor networks.

It achieves a higher filtering capacity and filters out more false reports than others in dynamic net - work.

3) Hill Climbing increases the filtering capacity of our scheme greatly and balances the memory requirement among sensor nodes.

8. CONCLUSION

In this paper, we propose a dynamic en-route quarantine scheme for filtering false data injection attacks and DoS attacks in wireless sensor networks. In our scheme, each node uses its own auth-keys to authenticate their reports and a legitimate report should be endorsed by nodes. The auth-keys of each node form a hash chain and are updated in each round. Secure routing is vital to the acceptance and use of sensor networks for many applications, but we have demonstrated that currently proposed routing protocols for these networks are insecure. We leave it as an open problem to design a sensor network routing protocol that satisfies our proposed security goals. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography alone is not enough. The possible presence of laptop-class adversaries and insiders and the limited applicability of end-to- end security mechanisms necessitate careful protocol design as well. The cluster-head disseminates the first auth-key of every node to forwarding nodes and then sends the reports followed by disclosed auth-keys. The forwarding nodes verify the authenticity of the disclosed keys by hashing the disseminated keys and then check the integrity and validity of the reports using the disclosed keys. According to the verification results, they inform the next-hop nodes to either drop or keep on forwarding the reports. This process is repeated by each forwarding node at every hop.

9. REFERENCES

1. Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler. Wireless sensor networks for habitat monitoring. In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
2. Braginsky and D. Estrin, “Rumor routing algorithm for sensor networks,” in Proc. WSNA, 2002, pp. 22–31.
3. Chris Karlof, Naveen Sastry, David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. ACM SenSys 2004, November 3-5, 2004.
4. K. Ishida, Y. Kakuda, T. Kikuno, A routing protocol for finding two node-disjoint paths in computer networks, in International Conference on Network Protocols, 1992, pp.340–347.
5. Karlof and D.Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” in Proc. 1st IEEE International Workshop Sensor Netw. Protocols Appl., 2003, pp. 113–127.
6. L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. ACM CCS, 2002, pp. 41–47.
7. N. Bulusu, J. Heidemann, and D. Estrin, “GPS-less low cost outdoor localization for very small devices,” IEEE Personal Communication. Mag.,
8. S. Capkun and J. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in Proc. IEEE INFOCOM, 2005, vol.3, pp. 1917–1928.
9. Sencun Zhu, Sanjeev Setia, Sushil Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In The Proceedings of the 10th ACM conference on Computer and communications security 2003.
10. T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, “Rangefree localization schemes in large scale sensor network,” in Proc. ACM MobiCom, 2003, pp. 81–95.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and 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

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