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 2401 Cities in 155 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

CHIEF PATRON

FOUNDER PATRON

CO-ORDINATOR

ADVISORS

EDITOR

EDITORIAL ADVISORY BOARD

ASSOCIATE EDITORS

TECHNICAL ADVISOR

FINANCIAL ADVISORS

LEGAL ADVISORS

SUPERINTENDENT

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Weinvite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing,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

WSN BASED ROBUST GROUND TARGET TRACKING FOR PRECISION GUIDED MISSILES

SANTANU CHATTERJEE
SCIENTIST
RESEARCH CENTRE IMARAT
DEFENCE RESEARCH & DEVELOPMENT ORGANISATION
HYDERABAD

SANTU SARDAR
SCIENTIST
RESEARCH CENTRE IMARAT
DEFENCE RESEARCH & DEVELOPMENT ORGANISATION
HYDERABAD

SOUMYADEEP BISWAS
SCIENTIST
RESEARCH CENTRE IMARAT
DEFENCE RESEARCH & DEVELOPMENT ORGANISATION
HYDERABAD

SANDIP ROY
ASST. PROFESSOR
ASANSOL ENGINEERING COLLEGE
ASANSOL

ABSTRACT

Ground based target tracking using low cost sensor based network, for Precision Guided Missiles (PGM) is very much effective for targets locating and precision guidance than traditional ways. Today PGMs depend heavily on GPS for location and navigation, also adding some advanced sensors for terminal target identification and guidance. Advances in inertial navigation systems (INS) also have added to the precision of weapons now deployed. But to enhance the precision of precision strike weapons in a cost effective way we are proposing distributed wireless sensor network (WSN) based target locating and precision guidance for PGM. Compared to the traditional ways, it has high precision, reliability, and also it can cope with the group targets with no duplication. For real time performance we have considered energy consumptions, computational overheads, new node deployments as well as security related challenges of the sensor networks. Further, our scheme is secure against different types of sensor network related attacks. The simulation results of our scheme ensure that our scheme can track, detect and classify targets in a timely and energy efficient manner.

KEYWORDS

PGM, GPS, INS, Distributed wireless sensor networks, target locating, authentication, security.

1. INTRODUCTION

Precision has always been recognized as an important attribute of weapon development. Accuracy of aim is one of the five recognizable attributes of weaponry, together with range of action, striking power, volume of fire, and portability. Now a new definition has emerged in warfare to describe munitions that can strike a target with extraordinary if not precise accuracy. Precision means that a projectile is self locating and maneuvers to its target. Precision weapons may be too costly to field in sufficient numbers to facilitate routine training, their effectiveness is limited to specific target types and engagement criteria and they lack the essential capability of delivering sustained physical and psychological shock that is intrinsic to dominant maneuver warfare.

Presently PGM type weapons utilize GPS/INS and seeker technologies for guidance to ground targets. GPS/INS systems work by acquiring position and velocity information and maneuvering to given target coordinates entered before release. By using seeker technology, target-tracking techniques are employed to guide to the final target. Potentially, missile seekers is used to view the area and send the images back to the planners, who could then take necessary action in regard to potential threats in that area. The missile would then continue on its flight path and strike its intended target. This would provide planners with a set of precision engagement tools in a rapidly changing threat environment. There is no doubt that Seekers bring relatively high accuracy than other traditional guidance system, for moving/ moveable targets but also it require much higher cost and greater mission planning, power, and cooling requirements. The ability to attack this class of targets without the expense and issues associated with seekers with greater accuracy is desirable. In this paper we presents a concept for precision guidance against moveable ground targets by using wireless sensor networks for implementation in air-launched munitions. Here, we try to address those problems and want to present a practical solution of WSN based target tracking in PGM.

A WSN is a system of spatially distributed sensor nodes with a goal to produce globally meaningful information from locally collected data. The nodes communicate wirelessly, operate autonomously and perform cooperative actions. In order to make good use of the locally collected data, nodes have to collaborate with each other and should form a network to perform any common application.

Now, Wireless Sensor Network is an absolutely necessary part of the C4ISRT (command, control, communication, computing, intelligence, surveillance, reconnaissance and targeting) system. WSN has the characteristics such as rapidly deployment, self-organized, good concealment and high fault tolerance that made it suitable for military usage.

Each sensor node in the WSN is battery powered and equipped with a low-power microcontroller, a radio transceiver, and sensor arrays. The onboard processor has limited memory and processing speed and a short sensing range. To overcome these challenges, we need the network to intelligently distribute the task of target tracking among the nodes and select the best sensor node for target tracking.

A sensor node is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. Typically, the transmissions between the sensors take place by short range radio communications. The base station is computationally resource-rich whereas the sensor nodes are resource-starved [2]. Each of the deployed sensor nodes has the capabilities to collect data and route data back to the base station. Usually, data are routed back to the base station by a multi-hop infrastructure less architecture through sensor nodes.

In this paper we aim to design and analyze target tracking and precision guidance based on wireless sensor network. Here for target co-ordinate determination triangulation method is used and we also consider the problems associated with multiple target determination , overlapping nodes, trajectory generation, detection areas before and after movement of targets, optimization technique to determine the optimal launch position of the daughter missiles and also various kind of security threats involved in wireless sensor networks. We analyze the performances of our scheme, using both theoretical and simulation environments and get a satisfactory result.

The rest of the paper is organized as follows. The next section gives a short description of the conventional target tracking procedures in PGM. Section three describes our proposed scheme of target tracking for PGM sing wireless sensor network (WSN), its security challenges and proposed solution and the experimental results. Conclusions from the current work and its scopes are elaborated in the last section.

1.1 MOTIVATION

Recently Y. Hu [1] has published his research on the targets locating and precision guidance of a kind of missile based on WSN. Though that paper is one of the pioneers of the research on WSN based target tracking for missile technology but it also suffers from some unrealistic ideas. In that paper author has not considered any base station that means sensor node directly transmit data to mother missile which will be in 3000m to 4000m height. Also he has not considered any security solutions for the networks which are very much required.

1.1.1 Problems associated with the traditional system in target tracking

There exist a few traditional technologies which have been implemented for target locating in a PGM type weapons. These include GPS/INS systems, seeker technology and auto-homing semi auto-homing systems. All of them suffer from some serious drawbacks as listed below:

- Using GPS/INS systems, the position and velocity information of the target needs to be entered before the missile release. This kind of systems lack in precision and accuracy for a frequent moving target.
- Seeker technology provides relatively high accuracy in target tracking but it demands much higher cost and greater mission planning, power, cooling requirements etc.
- In an auto-homing system, sender and receiver are installed in a sub-missile. Hence, the missile controlling process gets complicated and more energy is consumed. In semi auto-homing system, the sender is placed somewhere to cooperate with the missiles. is much lighter, but it is more depend on the sender. If the sender is destroyed, the missile will be lost.
- The auto-homing and semi auto-homing system cannot detect group targets and suffer from duplication of resource or even failure of the task.

1.1.2 Advantage of Using WSN based target locating for PGM application

A WSN based system for target locating and precision guidance is more promising in compared to the traditional techniques. Here, a large number of small computing nodes, called sensors or motes, are scattered in the sensor field or battlefield for the purpose of sensing information of the targets. The nodes can transmit those sensing information to either the nearby base station or directly to the mother missile for further processing.

A WSN based system has many advantages.

First, the nodes are dynamically deployable. We can easily deploy new nodes in the target field which can safely communicate with the existing nodes. This is quite necessary because in a hostile environment, older nodes can be compromised in many ways. Some robust access control protocol need to be implemented for dynamic addition of nodes.

Second, the nodes of WSN are self-organized. There no need to maintain a centralized control over the network.

Third, Battle field is a movable and multi-target environment. A WSN based system can help missiles attack group targets with no duplication and miss. Also this kind of system can provide higher precision over the traditional systems. Fourth, as the WSN based system have high Fault Tolerance, it is more suitable for military usage [22].

Fifth, the WSN based systems have low cost, low power, small volume and high redundancy. These make a WSN based system more reliable and more effective to apply to targets tracking in PGM than traditional systems [23].

1.1.3 Security requirements: Need of security in the system

In military application, wireless sensor networks operate in public, hostile and uncontrolled area. Before the sensed data reaches to the base station or to the mother missile, it is prone to different types of malicious attacks. Hence security is a major challenge in WSN based target tracking applications.

First, wireless communication is always under different threat realized over a broadcast medium. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject, and alter the transmitted data

Second, sensor networks work in an insecure environment. Adversaries can easily execute lot of harmful operations in the system such as stealing nodes, recovering their cryptographic material, pretend as authorized agent etc.

Third, Sensor nodes have limited computation, memory and energy resources. Adversaries can repeatedly send packets to drain a node battery and waste network bandwidth. In this resource-sensitive environment, secure transmission of sensitive digital information over the sensor network is quite essential.

Generally Wireless Sensor Networks are vulnerable to various types of attacks. In WSN based target locating for PGM application, we found some of them are very crucial. On the other side, few attacks are quite trivial and can't do much harm in our proposed system. A good understanding and recognition of possible attacks and threats will help us to build the required security protocol for this system. A WSN based target locating system is susceptible to the following type of attacks:

- Replay attack: Here an attacker spies or may intercept the conversation between the sender and receiver and takes the authenticated information.
- Forgery attack: A legal user of the system can launch a forgery attack against the WSN by eavesdropping and masquerading.
- Node compromised attack: Here attacker can steal all the data stored in any compromised node's memory and with that attacker try to get the cryptographic information in the network
- Sybil attack: In Sybil attack a malicious node illegally forges an unbounded number of identities. To overcome the problem of Sybil attack, unique identity of each node is required.
- Insider attack: In this attack any genuine user attacks the system for a different application for which he has no access permission.
- Worm hole attack: In this attack a malicious node tunnels to packets received in one part of the network and replays them in a different part of it.
- Many logged-in users with the same login-id attack: Systems which maintain a password-verifier table to verify user login are usually vulnerable to many logged-in users with the same login-id attack.
- Denial-of-service attack: Here an attacker tries to block the messages from reaching the base station as well as to other nodes in the sensor network.
- Withstand false reports injection attacks: An attacker may try to inject false reports into the sensor networks. An access control protocol must prevent external parties from injecting reports into the existing sensor networks.
- Withstand man-in-the-middle attacks: An access control protocol must protect the man-in-the middle attack from an adversary.

Resilience against node capture attacks: The resilience against node capture attack of an access control scheme is measured by estimating the fraction of total secure communications that are compromised by a capture of some sensor nodes not including the communication in which the compromised nodes are directly involved. An access control scheme must be highly resilient against node capture attacks.

1.1.4 Type of security is required for the system

To design a dependable and secure WSN based target locating system of PGM, we must implement two fundamental security issues.

First, in our system, either the ground base station or the mother missile acts as the user. A battlefield may contain many adversary missiles projected by the enemies. These missiles can pretend to be a real user and try to access the sensor node information. Here proper User authentication is essential for allowance of sensed data only to privileged users. But as the user is fixed and limited that is the base station or the mother missile so in this case we are not considering any traditional user authentication protocols used for WSN.

Second, Access control among sensor nodes is mandatory. This allows new sensor nodes to join dynamically in a secured way with the old valid nodes in the battlefield. An access control needs to accomplish the following two tasks:

- Node authentication: Through authentication a deployed node needs to prove its identity to its neighbor nodes and also to prove that it has the right to access the sensor network.
- Key establishment: Shared keys must be established between a deployed node and its neighbor legitimate nodes to protect communications, after successful authentication between them.

1.1.5Functionality Requirements

Scalability: A sensor network consists of a large number of nodes spread randomly throughout deployed area. Managing all these sensor nodes becomes a very difficult task. The number of nodes depends on the application. Sometime increasing the number of sensors in an area leads to better tracking results, but it is also true that beyond a critical threshold increasing the number of sensors does not improve the location precision in tracking. Hence, the placement of the sensors in the deployed area should be so as to maintain a balance between number of sensors and coverage required. But in our case deployment of sensor in territory is a difficult task. Random deployment is the only solution so some of the sensor may lose or damage at the time of deployment also. Taking care of this entire conditions secure WSN based target tracking system should be developed. Even at the time of authentication and key establishment between sensor nodes new node deployment phase need to be considered. Scalability is a essential functional requirement for our proposed scheme.

Stability:

As sensors are likely to be deployed in hostile environments so their failure is an issue forever. The network should operate well without supervision. Sensor networks instead are deployed in a very ad hoc manner (e.g. thrown down at random from an aircraft). Nodes are damaged and fail due to limited power available with them. The networks have to be able to overcome node failures and be able to reconfigure themselves. Considering such sensor nodes should establish an ad hoc network amongst themselves. Thereafter, different application instances running on each node can communicate with each other and the network should be stable and up for all the time.

1.1 THREAT MODEL

As in this paper we have proposed WSN based target tracking so security and attacks inside the WSN need to be addressed. For that purpose in our proposed protocol, we make use of the standard Dolev-Yao threat model [24] in which two sensor nodes communicate over an insecure channel. In a similar fashion we assume that the sensor nodes or end-points cannot be trustworthy in general and the communication channel is insecure. Finally, we assume that an attacker can eavesdrop on all traffic, inject packets and reply old messages previously delivered.

In our proposed scheme, two assumptions are quite fundamental. First, the ground base station which receives the sensing information from the nodes is trustworthy and not to be compromised in any situation. Second, the sink node of the mother missile should never be compromised as it receives the processed information from the ground base station or it accumulates the information directly from the sensor nodes. Thus, if an attacker compromises any sensor, he/she can extract all cryptographic information including the key materials, data and code stored on that node though. This is a big threat to the system as it is very easy for the enemies to steal sensor node from a captured battlefield.

1.2 OUR CONTRIBUTIONS

In this paper, we propose a new scheme for target tracking for precision guided missiles using wireless sensor networks.

Our scheme has the following important properties:

- This work addresses a real-world application for precision guided missiles using ground based wireless sensor networks.
- We investigate the functional challenges for implementing conventional target tracking methods used for PGM for moving targets.
- In this paper we also proposed security mechanisms for wireless sensor networks used specially for target tracking for PGM.
- We have also identified the challenges with respect to real time requirements and validate our design and analysis through simulation with few numbers of nodes.

1.3 ORGANIZATION OF THE PAPER

The rest of this paper is organized as follows. In Section 2, we review the conventional target tracking system. In Section 3, we briefly discuss the mathematical preliminaries needed to understand our proposed security protocols. Here, we also discuss the advantage of an ECC based system. Section 4 describes the related work done in the field of WSN based target tracking system. In Section 5 we describe our proposed scheme. Section 6 presents our proposed solution for WSN based PGM and models the experimental results. Finally, we conclude the paper in Section 7.

2 CONVENTIONAL TARGET TRACKING IN PGM

The two widely used conventional techniques for engaging air-to-surface missiles on to ground target are active radar homing and semi-active radar homing [3]. In active homing the missile can illuminate the target with radar signals and track it autonomously by the help of a radar transceiver present onboard the missile, shown in fig 1. In semi-active homing missiles the targets are illuminated by a higher power transmitter usually located on the ground, and the reflected signals from the target is used to home the missile on to the target as shown in fig. 2.

In addition to this, both types can employ a passive radiation homing, if the target does attempt to jam them using some kind of ECM, they can in effect turn into an anti-radiation missile and home in on the target's radiation passively. Some advantages and disadvantages offered by the above two techniques are as listed below.

FIG. 1: ACTIVE RADAR HOMING

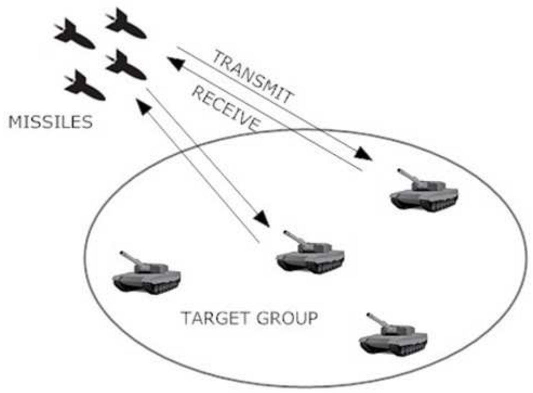
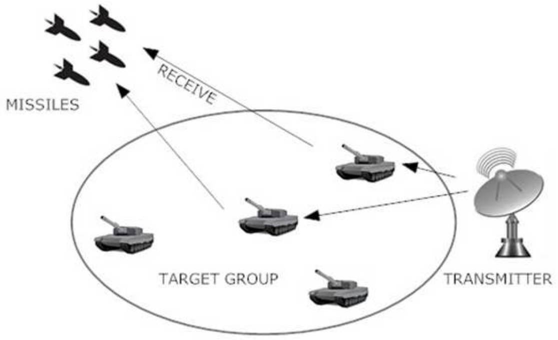


FIG. 2: SEMI-ACTIVE RADAR HOMING



- Active radar homing missiles has higher kill probabilities since the missile is approaching the target and the accuracy of tracking is increasing. But since the radar transceiver has to be small enough to fit inside a missile and has to be powered from batteries, therefore having a relatively low Effective Radiated

Power (ERP), its range is limited. Often it is used with other navigational systems like command guidance or Inertial Navigation System (INS) but it greatly increases the complexity and cost of the missile.

- The semi-active homing has reduced complexity in the sense that only a passive radar receiver is required onboard but it is dependent on the transmitter. If the transmitter is destroyed then the missile cannot be guided on to the target.
- In a scenario where a group of missiles is engaged for a group of targets, since there is no inter communication among the missiles to intimate their individual target engagement, there is a high probability that multiple missile may lock on to the same target while some target within the kill range of the missiles are not hit.

3 MATHEMATICAL PRELIMINARIES USED FOR CRYPTOGRAPHY AND SECURITY FOR WSN

In earlier days, either RSA cryptography system [17] or Diffie-Hellman [12] key agreement were mostly used for providing security of traditional networks. But in a resource constrained domain of sensor networks, these traditional ideas are not suitable implement. The sensor nodes are comprised of limited energy resources, limited computation and communication ability and limited bandwidth [1, 8]. Along with these, sensor networks are dynamic in nature and post-deployment network configuration is not possible to decide a priori. Therefore new cryptographic ideas are needed.

In a WSN based target locating for PGM application, new sensor nodes needs to be dispersed in the battlefield quite frequently. In this scenario, conventional key pre-distribution schemes [10, 11,13,14] are very difficult to use. Whenever a new node joins the existing sensor network, they demand an updating of all the old secret keys and broadcasting messages. This is quite an impractical idea.

A sensor network must establish a suitable access control protocol to prevent the malicious nodes from joining it. The protocol should also include a dynamic key establishment mechanism to help new valid nodes to establish shared keys with its neighbors for a secure communication. In 2007, Zhou et al. [16] proposed an access control protocol based on elliptic curve cryptography (ECC) for sensor network which is more efficient than those algorithms based on RSA. Compared to RSA, ECC can achieve the same level of security with smaller size key. For examples, 160-bit ECC provides comparable security to 1024-bit RSA and 224-bit ECC provides comparable security of 2048-bit RSA [17]. It was pointed out in [18] that in wireless sensor networks, the transmission energy consumption rate is almost three times greater than the energy consumption rates for computing. Therefore, the packet size and the number of packets in transmission play a crucial role in the performance while designing an access control protocol in sensor networks. It is noted that if a node is preloaded with the certificate by the base station, then verifying RSA signature in the certificate takes less time than that for ECC signature verification in the certificate, since the signature will be generated in offline by the base station prior to deployment of sensor nodes in the target field. However, compared with a 1024-bit RSA signature [15], if we use ECC based signature [19, 20] in certificate, then we require only 320-bit signature when 160-bit ECC is used in the proposed scheme. These motivate us to use ECC instead of RSA in our proposed access control scheme so that we base station certainly achieve much more energy and bandwidth savings. Our scheme uses the symmetric key cryptographic techniques along with ECC to achieve better communication and computational efficiency.

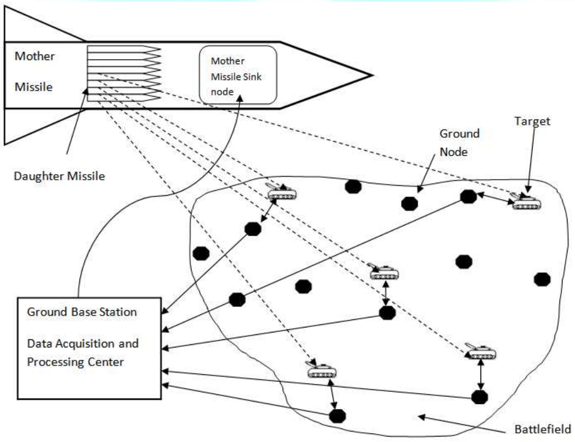
A cryptographic system using elliptic curve [21] can be designed as follows:Consider the equation Q = kP, where Q, P ϵ Ep(a, b) and k < p. It is easy to calculate Q given k and p, but it is relatively hard to determine k given Q and P. The problem is known as Elliptic Curve Discrete Logarithm Problem (ECDLP). In ECC a base point or generator point G = (x1, y1) of order n in the elliptic group of points Ep(a, b)is identified. then user choose the smallest integer value n for which they have nG = O where O is the zero point. The case is that for Given G and kG, it is computationally hard to find out k so an attacker needs to compute k to break this scheme. This practically is an infeasible task.

4 THE PROPOSED SCHEME

Target tracking for PGM using WSN: In the proposed WSN system, a number of tiny sensors are dispersed near the adversary's battle field. These sensors work as nodes in the system. The nodes accumulate information of the targets, and send the raw signals to the ground based base station. The base station processes the signals of the individual nodes to determine the number of targets and their locations. The sink is on the mother missile. The information of the targets is sent to the sink from the ground base station. After computation by the control system, each sub-missile is assigned a particular target, which maybe the nearest target or the target considering all other sub-missiles so as to best finish the whole task. The structure is shown in Fig. 3.

With broad scale of nodes, the information content is very large. The position of the group targets can be detected all together by the WSN system, and the attacking plan can be settled before the sub-missiles are released, so that each sub missile has its unique destination, with no duplication and waste of power. Therefore, the fatal problem of the traditional ways is resolved.

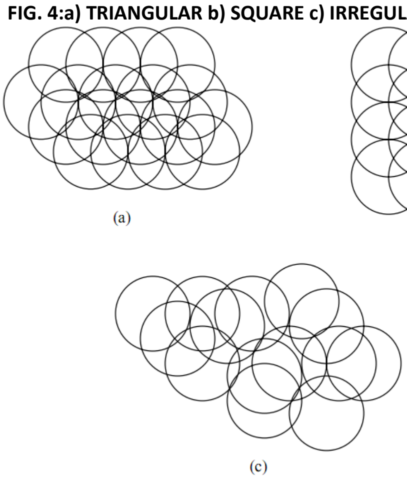
FIG. 3: STRUCTURE OF WSN FOR TARGET LOCATING AND PRECISION GUIDANCE



As the nodes are very small and ulterior, it can be put very close to the enemy's battle field, so more accurate data can be got compared to the traditional method. The number of nodes can be very large. Therefore the reliability is increased at the same time because if one node fails, others are still working.

We visualize a heterogeneous, hierarchical sensor network that is composed of a static backbone of sparsely placed high capability sensors called CHs and moderately to densely populated low-end sensors whose function is to provide sensing information to CHs upon requests [4]. Because of the limited mobility nature of sensors, the calibration process of sensor locations is executed only once when the network is deployed. A CH volunteers to become active when it detects that the strength of a received radio frequency (RF) signal exceeds a pre-determined threshold and the signal matches one of the signal patterns which the system intends to track. The sensors can be deployed in any facility or area which has to be sensed in three main types [5]. It can either be 1) triangular sensor deployment, 2) square sensor deployment or 3) irregular sensor deployment Fig. 4.

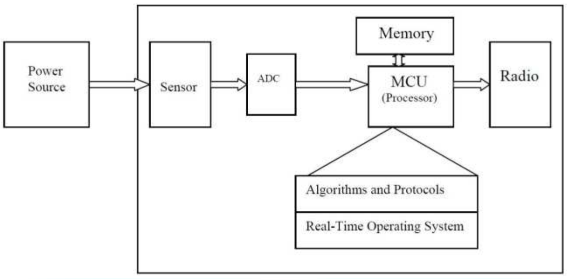
FIG. 4:a) TRIANGULAR b) SQUARE c) IRREGULAR NETWORKS



For our case, we have to choose irregular sensor deployment as the sensor nodes will be distributed irregularly in the battlefield. A sensor node should consist of four sub-systems [5] as shown in Fig. 5.

- A computing subsystem: In a sensor node, the microprocessor (microcontroller unit, MCU) is responsible for functions such as control of sensors and execution of communication protocols. Since these functions consume a lot of energy, an MCU operates under various modes of energy consumption.
- A communication subsystem: This comprises of short range radios used to communicate with neighboring nodes and the outside world, these devices operate under the Transmit, Receive, Idle and Sleep modes having various levels of energy consumption. The maximum energy consumption is in the first two modes and if the sensor is not performing any function, it should be shut down rather than putting in idle mode.
- A sensing subsystem: Low power components can help to significantly reduce power consumption here since this subsystem (sensors and actuators) is responsible for the sharing of information between the sensor network and the outside world.
- A power supply subsystem: Since a battery supplies power to the sensor node, the amount of power being drawn form it is constantly being monitored. The lifetime of a battery can be increased by tuning it on and off depending on the functionality of the node in question. This process should ideally be automated.

FIG. 5: SYSTEM ARCHITECTURE OF A WIRELESS SENSOR NODE



The sensor nodes may not need identities (e.g. an address). Applications should focus on the data generated by the sensors. Individual sensor nodes in a network can perform the functions of information gathering, collecting and storing and forwarding of information/data on request from neighboring nodes. This is in contrast to a centralized structure in the case of routers that facilitate node-to-node packet switching in traditional networks. Individual sensors report their data to a central node, which then performs the computation required for the application. This centralized structure is a bad choice for several reasons: it provides a single point of failure, it can be energy inefficient, and it doesn't scale to large networks. Thus, localized algorithms are better suited to sensor networks in which each sensor node communicates with neighboring nodes and computation is performed locally, yet the entire structure achieves a desired global objective. Since the sensors are physically distributed, it is not unnatural to design sensor networks using distributed algorithms. Furthermore, localized algorithms have two attractive properties. First, because each node communicates only with other nodes in some neighborhood, the communication overhead scales well with increase in network size. Second, for a similar reason these algorithms are robust to network partitions and node failures.

As an alternate to the trilateration technique some other techniques [6] have also been proposed. They are: infrared, ultrasound and Radio. In our case, radio wave is considered for locating the target within the region of interest of a node because it provide a better approximation for location detection because of the ability of these waves to penetrate various materials. Instead of using differences in arrival times as in Ultrasound, these systems utilize signal strength to measure the location.

To reduce budget, some system only set GPS receiver to a small part of nodes, the neighbor nodes localize themselves based on pair wise distance or angle [9]. In fact, here all the nodes do not have to carry GPS receiver, because for the missile to finish the attacking task, the information needed is actually the relative location of targets to each missile. The nodes only have to measure the distance and angle between itself with missile and with target, and the distance and angle between the missile and the target is calculated with a simple triangular law. So the budget can be greatly reduced, and the saved budget can be used to reinforce the detect precision and communication ability.

5 THE PROPOSED SOLUTION

5.1 OUR SECURITY PROTOCOL

As for our proposed scheme wireless sensor networks will operate in uncontrolled area or battlefield, hence the security is a major challenge in sensor applications. Because sensed data of sensor nodes is prone to different types of malicious before reaching base station. Security is one of the most difficult problems facing these networks. First, wireless communication is difficult to protect since it is realized over a broadcast medium. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject, and alter transmitted data. Second, since sensor networks may be deployed in a variety of physically insecure environments, adversaries can steal nodes, recover their cryptographic material, and pose as authorized nodes in the network. Third, Sensor networks are vulnerable to resource consumption attacks. Adversaries can repeatedly send packets to drain a node battery and waste network bandwidth. In these and other vital or security- sensitive deployments, secure transmission of sensitive digital information over the sensor network is essential. The use of encryption or authentication primitives between two sensor devices requires an initial link key establishment process, which must satisfy the low power and low complexity requirements.

Generally, without involving the gateway node users preferred to access directly the sensed data so real-time transmission of sensed data is required. User authentication and authorization and access control are mandatory for allowance of sensed data only to privileged users through base station.

As here base station is only involved in communication with user that means the mother missile so in this case for each user hash value of its password with a time-stamp along with its identity should be stored in the base station. So at the time of flight that mother missile can be genuinely recognized by the base station as well as hash of the base station id with the mother missile times-tamp along with identity should besend to the mother missile for mutual authentication. So if some other user tries to intercepts the message they will not be successful.

For access control we want to use simple dynamic access control protocol proposed by Huang et al. [7]. Here we want to use an energy efficient and low computational overhead dynamic access control protocol in WSN using hash functions [8] and XOR ($\oplus$) operations. In this protocol the base station generates different secret keys for all the neighborhood nodes and preloads each secret key ki , one way hash function, node identity Ni and boot strapping time of the node Ti to each node i. After that base station generates pair wise secret keys Sij by computing the XOR ($\oplus$) of the hash values of one node's identity with other node's secret key, for each pair of nodes i, j in the sensor network. Here

$Sij = H(ki , Nj) \oplus H(kj , Ni)$.

Later this pair wise secret keys Sij for each pair of node i, j are broadcasted.

In authentication and key establishment phase any node i first computes the hash value of its own node identity with other node secret key H(kj, N) by using XOR ($\oplus$) operations. It also generates a random number ti and computes hash value zi of that random number with the previous computed hash value.

$zi = H(ti, H(kj , Ni))$.

Then send this with the generated random number and along with its node identity.

After receiving the message other node of the pair j computes the hash value Hj of its own secret key kj and identity of node i.

$Hj = H(kj , Ni)$.

Then it calculates the hash of Hj and the received ti. If this computed value matches with the received zi then node j authenticate node i as a legitimate node and similarly computes zj and a shared session key

$kij = H((H(kj , Ni) \oplus ti) \oplus ((H(ki , Nj) \oplus tj))$.

Then similar to node i node j also send zj, tj, Nj to node i. After receiving the message from node j, node i verify zj in a similar manner and after successful verification computes shared session key kij and another hash value

$yij = H(kij , ti \oplus tj)$

and deliver yij to node j for establishing mutual authentication.

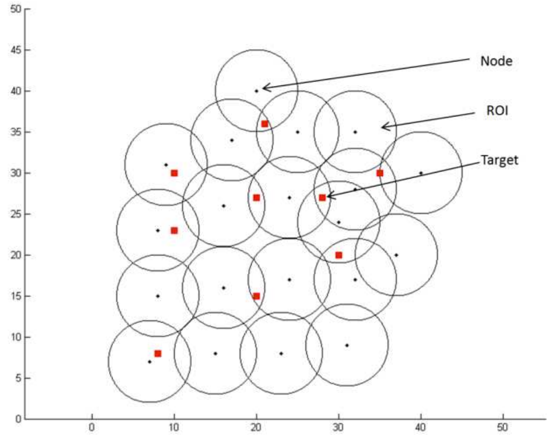
Node j checks the authenticity of yij and if it holds then connection will be established between these two nodes. For new node addition this protocol follows the same authentication and key establishment phase so other information in existing node need not to be updated. By using this protocol we can achieve our desire security of WSN for PGM target tracking.

5.2 EXPERIMENTAL RESULTS

In order to verify that the WSN system can cope with the target locating and precision guidance mission with advantages of high precision and no duplication, simulation of a theoretic model of the task is done. Multiple sensors and targets are considered within the region of the battlefield. Every node has its own region of interest (ROI). If target falls within its ROI, the node will collect information about the target and send to the ground based base station. In the base station, the location of the target is determined.

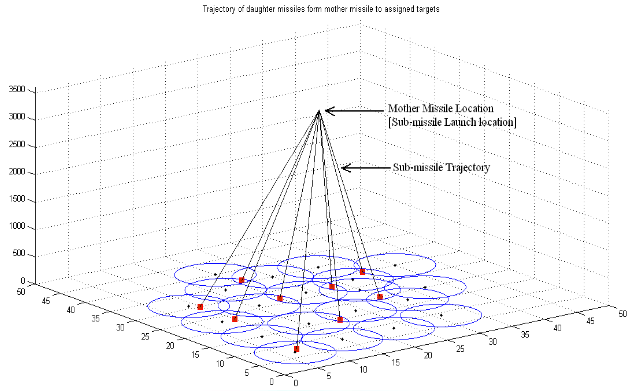
Nine different targets and twenty nodes are considered. The arrangement of the nodes and targets are shown in Fig. 6.

FIG. 6: NODES, THEIR ROIS AND TARGET LOCATIONS IN THE BATTLEFIELD



The circular region of interest (ROI) of a single ground node is taken to be 5 meter. For each ground node, if a target is in its ROI, it determines the distance of the target from the node and its angle with reference to a specific coordinate system. There can be scenario here multiple target may fall within single ROI or single target may fall in multiple ROI as the nodes are randomly distributed in the battlefield. To decrease the processing power of the individual node, each node computes only distance and angle of the target within its ROI and the raw data is sent to the base station. If multiple targets fall within single ROI of a node, the node sends information regarding each target. If single target falls in multiple ROI, each of the nodes corresponding to intersecting ROIs will detect the target separately. In that case, there is a chance of multiple instance of same target. To remove repetition of targets, target duplication removal algorithm is implemented in the base station. After the base station computes the coordinates of the nine targets, the target location information is sent to mother missile sink node to engage single sub-missile to single target. The mother missile is assumed to be 3500 meters above the battlefield. The total process is simulated and each of the nine sub-missiles are assigned individual distinct target and the targets are intercepted successfully as shown in the Fig. 7. These groups of nine targets are correctly detected by the set of ground nodes.

FIG. 7: TRAJECTORY OF SUB-MISSILES FROM MOTHER MISSILES TO THE TARGET



6 CONCLUSION

In this paper, we demonstrate the feasibility to design a complex real-time wireless sensor network for target tracking by PGM. We also analytically identify the challenges among system properties while meeting the real time requirements. We validate our design and analysis through simulation with twenty nodes. We contribute a set of tradeoffs that are useful for the future development of real-time sensor systems for target tracking by PGM. Given real-time constraints, a system designer can make guided engineering judgments on the system parameters such as the network density, the appropriate detection algorithm and the security and protocol settings for the sensor nodes in the network.

7 REFERENCES

1. C. W. Park, S. J. Choi, and H. Y. Youn, “ A novel key pre-distribution scheme with LU matrix for secure wireless sensor networks”, International Conference on Computational Intelligence and Security (CIS 2005), Springer-Verlag, Germany, LNAI. 3801, Part I, Dec. pp. 494-499, 2005.
2. D. Dolev and A. Yao. On the security of public key protocols. IEEE Transactions on Information Theory, 29(2):198–208, 1983.
3. D. Johnson and A. Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical Report CORR 99-34, Dept. of C & O, University of Waterloo, August 23, 1999.
4. D. Johnson and A. Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical Report CORR 99-34, Dept. of C & O, University of Waterloo, August 23, 1999.
5. D.W. base stationrman, P.S. Kruus, and B.J. Matt. Constraints and Approaches for Distributed Sensor Network Security. dated September 1, 2000. NAI Labs Technibase stationl Report No. 00-010.
6. Diffe Whitfield and Hellman M, “New directions in cryptology,” IEEE Transaction on Information Theory, Vol. 22, 1976, pp. 644-654.
1. F. Akyildiz, W. Su, Y. Sankarasuramaniam, and E. Cayirci, “ A survey on sensor networks”, IEEE Communications Magazine, Vol. 40, no. 8, pp. 102-114, 2002.
7. H. Chan, A. Perrig and D. Song, “Random key pre-distribution schemes for sensor networks”, IEEE Symposium on Security and Privacy, pp. 197-213, 2003.
8. H.-F. Huang and K.-C. Liu, “A new dynamic access control in wireless sensor networks,” pp. 901–906, 2008.
9. I.F. Akyildiz, W.Su, Y. Sankarasubra-maniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, pp. 393–422, 2002.
10. L.Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks”, Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 41-47, 2002.
11. Liming Sun, Jianzhong Li, yu Chen, and Hongsong Zhu, Wireless Sensor Network, Beijing: Tsinghua University Press, Aug. 2005 (In Chinese).
12. R.L. Rivest, A. Shamir, and L.M. Adleman, “A method for obtaining digital signatures and public key cryptosystems,” Communications of the ACM, vol. 21, pp. 120-126, Feb. 1978.
13. S. hash standard, fIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995.
14. S. J. Choi, and H. Y. Youn “An efficient key pre-distribution scheme for secure distributed sensor network”, The 2005 IFIP International Conference On Embedded And Ubiquitous Computing (EUC’2005).
15. S. Vanstone. Responses to NIST’s proposal. Communications of the ACM, 35:50–52, 1992.
16. T. A. Malik, Target Tracking In Wireless Sensor Networks. Maharshi Dayanand University (India), 2005.
17. T. A. Malik, Target Tracking In Wireless Sensor Networks. Maharshi Dayanand University (India), 2005.
18. W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd Edition, Prentice Hall, 2003.
19. W.-P. Chen, J. C. Hou, and L. Sha, Dynamic Clustering for Acoustic Target Tracking in Wireless Sensor Networks, 3rd ed. IEEE Transactions on Mobile Computing, 2004.
20. X. Meng, “Guide and control system theory of matlab,” in Beijing: Beijing Insitute of Technology Press, February 2003.
21. Y. Hu, “Research on the Targets Locating and Precision Guidance of a Kind of Missile Based on WSN,” IEEE Transaction, 978-1-4244-5273-6/09/26.00 © 2009 IEEE.
22. Y. Zhou, Y. Zhang, and Y. Fang, “Access control in wireless sensor networks”, Ad Hoc Networks, Vol. 5, pp. 3-13, 2007.
23. Zhen Feng, “Region Based Localization in Wireless Sensor Networks”, Dissertation, Huazhong University of Science and Technology, Oct. 2007 (In Chinese).

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

ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, ECONOMICS & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF
ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF
ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF