I. J. Computer Network and Information Security, **2017, 12, 36-44**
Published Online December 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.12.05

Monitoring of Military Base Station using Flooding and ACO Technique: An Efficient Approach

Abdus Samad
University Women’s Polytechnic, F/O Engg. & Tech., AMU, Aligarh, India
E-mail: asamad.uwp@amu.ac.in

Mohammed Shuaib
Dept. of Computer Science, Jazan University, Jazan, KSA
E-mail: talkshuaib@gmail.com

Mohd Rizwan Beg
R B Group of Institutions (RBGI), Agra, India
E-mail: rizwanbeg@gmail.com

Received: 22 January 2016; Accepted: 12 September 2017; Published: 08 December 2017

Abstract—Rapid development of Wireless sensor network led to applications ranging from industry to military fields. These sensors are deployed in the military base station such as battlefield surveillances. The important issues like security & DoS attacks play crucial role for wireless sensor network. Due to the limitations of resources, traditional security scheme cannot be employed efficiently. Therefore, designing a framework that can operate securely using smart intelligence technique is the best option. In this paper, an efficient way of detecting an intrusion using Flooding and Ant colony is proposed. The flooding technique enables the master agents to track the activity of intruder tampering the part of the network. The ACO identifies the path followed by the nodes and also the intruder, who wants to jam the whole wireless sensor network. The architecture strategically enables the Bait agents to detect the intruders threatening the network. The proposed framework is designed for the military station. It helps the base station to detect the intrusion and decide whether the activity is normal or terrestrial and send the signal to the nearest missile station situated near the intrusion location and destroy it in minimum time. The process of detecting the intrusion earlier not only helps to learn future attacks, but also a defense counter measures.

Index Terms—Bait agent, Master agent, Intrusion detection, Flooding Ant Colony, Intrusion detection, DoS attack.

I. Introduction

Protection and security of the network is the main goal of the researchers and several researches in this direction have been reported in the literature. The various approaches include the potential of Artificial Intelligence, incorporating the biological system such as ACO and detection and defense from the DoS attacks [1], [2], [3].

The security of ground base station is one of the major area where different system of systems (SoS) architectures are applied; a set of independent heterogeneous networked systems cooperate for a common goal [4]. These SoS architectures consists of minimum a Base Station, a set of launchers and at least one sensor with a base station monitoring Unit. These units integrate all Command, Control, Computing, Communications and Intelligence [3], [5].

The wireless sensor network (WSN) consists of a number of spatially distributed nodes that consist of sensors, processing elements and low power radio channels that provide wireless communication with each other as well as with the base station. The base station has larger power with high data rate as compared to sensor nodes. However, sensor node perform specific task for which they are designed at a particular location. The base station on the other hand plays the greater role and performs operation such as information gathering, node activation and networks. They also provide interface with other sensor networks. The advantages of WSNs technologies are remarkable that provide in an expansive way to install a network and greatly contributed worldwide in WSNs applications [6]. The military application such as battlefield is an important example where WSNs are widely used.

Generally, thousands of sensor node connectivity work to sense various physical and environment characteristics. These sensors are arranged in the form of various clusters. Each cluster has a root node with a set of sensor. The cluster communicates well each other through route node or with a specialized node also known as a base station. WSNs is scattered in region where its installation is made to collect data through its sensor nodes. The most modern WSNs are bidirectional in nature to make communication both ways. They could be used to collect data from sensors transmit it to base station as well as transfer information from base station to sensors.

The resent growth in the security systems demands a secure, reliable and cost effective wireless sensor network to detect intrusion in the Base station. In this paper a new model of security and monitoring system is purposed which utilizes the concept of bait system in a dynamic way. Baits including ideal agents and a master agent are deployed which captures all the activities or data within the real application.

The rest of the paper is organized into eight sections. Section I is introduction. In section II, we describe the related work in detail. In section III, different types of attacks are discussed. Section IV describes some existing approaches. The proposed system is discussed in section V and VI. Section VII describes architecture of intrusion detection system and section VII concludes the paper.

II. Litrature Review

The development of sensor technology has become an important tool for modern military applications. The important issue while using this technology is how to install these sensors in the remote environment. There are different approaches to deploy these sensor networks in the battlefield depending upon the knowledge of the environment. If sufficient knowledge is available then sensors can be deployed in strategic manner where part of sensor can be used as bait for intruders. On the other hand in the absence of suitable information these sensors can be employed randomly [3], [7], [8].

There are many intrusion detection frameworks to solve the problem of intrusion. To prevent the intrusion detection, Muraleedharan [3] proposed an Ant Colony Optimization based intrusion detection system. It is simulated and showed that the cognitive model has a performance of 90% and above during all run, whereas, dynamic and static model has 75% and 60 % performance respectively. The lifetime in cognitive model is reduced by 20%, whereas its reduction in static and dynamic is 10% and 20% respectively.

Another approach is based on SWARM architecture for ground based air defense system in which the author purposed several distributed algorithm focused exclusively in the optimization of launcher SWARM performances. Those were based in non- cooperative competition in term of probability of intercepting or killing a threat. However, the missile launching mechanism is made in a static way [2], [5], [7].

Similarly, in [3] the authors purposed several cooperation and distributed algorithms for SWARM architecture applied to ground based air defense, however, it doesn’t handle the threats when they are out of range.

The wireless sensor network (WSN) composed of numerous sensors and can adapt to extreme environment and have characteristics of small, low cost wireless communication sensors. These (WSN) also be deployed in adversary area, so the nature of communicating channels of (WSN) between sensor nodes makes node communication vulnerable to a variety of attacks. Due to constraints in its resources, WSN’s are especially sensitive to Denial-of-Services Attacks (DoS) [9]. A DoS attack is intent to prevent the normal use of network functions and communications [5], [10].

A plethora of many DDoS defense scheme is reported in literature. In [11] the author distributed types of DDoS attacks and their remedial actions. A number of approaches such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP flow analysis have been discussed. The various tools and software’s accustomed to handle DoS attacks in sensor networks are also discussed. The Connection Score scheme is another technique to overcome DDoS attacks that generally occurred at the application layer of TCP modified [12]. The connection is scored when attack occurs based on the available history and statistics analysis. These connections re-use resources which take lower scores and considered as adversary or malicious attacks.

The real-time PSD converter based on FGPA to prevent shrew DDoS attacks which are low rate TCP targeted attacks [13]. The system uses component-reusable auto-correlation (AC) algorithm and adapted 2N-point real-valued Discrete Fourier Transform (DFT) algorithm.

The researcher analyze various methods to prevent DDoS attacks based on traffic anomaly parameters, botnet flux identifications, neural networks, entropy variations, application layer DDoS defense and device level defense. Some traditional methods for instance trace back and packet filtering techniques are also discussed [14]. The intrusion prevention system handles DDoS detection and also analysis the role of network management systems to detect DDoS attacks with minimum losses [15]. The numerous information metrics that describe properties of network traffic data to the detection of low-rate and high-rate DDoS attacks are described [16]. All these matrices contain Shannon entropy, generalized entropy, Renyi’s entropy, Hartley entropy and Kullback leibler divergence. By the use of these techniques such as MIT Lincoln Laboratory, CAIDA and TUIDS DDoS datasets can check the effectiveness of each metric.

In [17] the researcher also discussed the Game-theoretic defense framework that explains communication among an attacker and a defender during a one-shot, non-cooperative, zero-sum game DDoS attack. The new method has proposed to detect DDoS attacks at application layer that considers detection of AL-DDoS attack in high traffic [18]. This method includes a Real-time Frequency Vector (RFV) and attacks can be recognized by investigating the entropy of application layer-DDoS attacks and flash crowds.

In order to obtain a secure, reliable and cost effective correct network to detect instruction a new security model is proposed. The proposed system initializes the concept of bait system in a dynamic way to monitor the overall security measures.

III. Types of Attack

Broadly attacks are classified into two categories based on methodology used known as active and passive attacks. When the attackers identify the security holes in the network and utilize those gaps to launch massive attacks they are termed as active attacks. In these attacks the attackers generally modify the packets, inject new packets or replicate information to gain advantage of security lapse. In passive attacks, the intruder always tries to extract crucial information of communication protocols and follow those information like normal sensors. In this way a large information come around the intruders through which secret or useful information could be extracted [19]. It is very different to identify the passive attackers in short span of time; however, active attacks are much stronger as compared to passive attacks.

The influence of such attacks appears in different ways which are listed in Table 1.

Table 1. Denial of Service Attacks by Protocol Layers

Protocol layer	Attacks
Physical	Jamming
	Tampering
Link	Collision
	interrogation
	Denial of sleep
Network	Replayed Routing
	Black Hole
	Sink hole
	Sybil
Transport	Flood
	Desynchronization
Application	Overwhelming sensors
	Path based DoS

A. Physical Layer

There are two types of attacks generally encountered at physical layer. These are:

a) *Jamming:* Jamming is a kind of attack which interferes with the radio frequencies that network's nodes are employing. Since, WSNs use radio based medium so there are more vulnerable to jamming. Jamming can interrupt minimal part of the network or it could be strong sufficient to interrupt the entire network [20]. An intruder may affect the entire network when the jamming sources are randomly distributed in the entire network.

Jamming attacks in WSNs: Jamming attacks can be classified as constant, depictive, random or reactive [21]. In constant jamming attack, packets are targeted and made correct during transmission between WSN nodes. However, these attacks are not significant, if attackers do not have compatible energy as targeted node. A deceptive jammer mix information in such a way that it look like legitimate traffic. On the other hand a reaction jammer only transmits a jam signal. Defense strategies such as frequency hopping and code spreading are required to protect the network. To identify the jamming attacks the jammed region are to be identified one safe region. The routing protocol must automatically route around jammed region. Another strategy for defending against jamming is to have nodes collaboratively identify the jammed region. Node tampering is another physical layer attacks that causes destruction of network.

b) *Tampering:* This is another physical layer attack in which an intruder can remove expensive data by having physical access to a node. The node may also be altered or converted into malicious node and could be used as controlling node. Defense strategy involves tamper-proofing the node's physical package. There are different approaches for identifying Jamming attacks in WSNs. Node deployed in secured area could be saved up to some extent; however, redundant nodes can be affected by this threat and then route traffic around it.

B. Link Layer

The collision and Interrogation are two types of attacks generally reported in link layer. When packets collide with each other, alteration in information at source and destination node appears. Therefore, differences in the checksum are obtained. Thus packet will be treated as invalid and discarded. An adversary may continually transmit messages in an attempt to generate large collisions in entire network. This requires retransmission of packets affected by the collision such as ACK or NACK control messages. With help of error correcting codes collisions can be avoided [5]. An attacker can consume a node's resources by frequently transmitting RTS requests to obtain CTS responses from a under attack node [5]. Anti replay protection and strong link-layer authentication are some defense strategies against such type of attacks [23].

Another link-layer threat to WSNs is the denial-of-sleep attack, which prevents the radio from going into sleep mode [24]. An attacker might choose to execute a denial-of-sleep attack over a simple jamming-based DoS attack on a WSN to limit the attack's duration.

C. Network Layer

a) *Replayed Routing Information:* In this case, an attacker may modify the routing information in order to disturb traffic in the network [25]. This type of disruption attracts traffic from particular node, may increase or decrease the routes or generates bogus/wrong messages.

b) *Black hole:* A black hole is a specific attack in which a node drops all messages it receives as if the node doesn't exist at all. An attacker may perform another form of attack by selectively forwarding only certain messages and simply dropping others which is denoted by grey holes [26].

c) *Sinkhole:* In a sinkhole attack, an attacker makes a compromised node look more attractive to nearby nodes by forging routing information [5].

d) *Sybil:* In this attack, a single node presents a variety of identities to all other nodes in the WSN. It may deceive other nodes, and hence routes made between valid nodes may possibly be between a valid node and compromised node.

D. Transport Layer

A very common form attack appeared at transport layer is to send a large number of common packets aimed at a single destination [27]. The most common packets used are: TCP, ICMP, and UDP. The huge traffic deluge caused by these packets leads the network to no longer be able to distinguish between legitimate and malicious traffic. Basically all available resources such as bandwidth are used up and nothing is left for legitimate use causing the users to be denied the service of the network.

De-synchronization is another type of attack detected at transport layer [26]. For example, repeatedly spoof messages to an end host causing that host to request the retransmission of missed frames. An attacker may degrade or even prevent the ability of the end hosts to successfully exchange data to instead waste energy which could otherwise be utilized by legitimate nodes in the network.

E. Application Layer

This type of attack is known as Overwhelm attack. It results in consumption of whole bandwidth and energy. Its effect can be reduced using Rate-limiting and efficient data aggregation algorithms. [28].

Path-based DoS attack is also belongs to application layer. It involves transferring bogus or replayed packets into the network at external or farthest nodes. Hence prevents valid nodes to transfer data to the base station. Anti replay protection and packet authentication can prevents these attacks [26]. This attack consumes network bandwidth and drains node energy. However, it affects only when particular sensor readings triggers communication and not applicable when sensor readings are sent at fixed intervals.

F. Denial of service (DoS) ATTACKS

In the previous section, a variety of possible attacks to sensor network is discussed. Since sensor nodes are deployed over a large geographical area therefore they are more vulnerable to any of these attacks [6].

Denial of service attacks also known as DoS attacks is the most common attacks to wireless sensor network security. These attacks use wireless communication links to starve the network legitimate traffic [29]. The DoS attacks do not attempt to destroy the complete system, however, the pressure of these attacks directly affect the functioning of the network users. Sometimes users are deprived of those services which are meant to be available with them. Often DoS attacks badly affect the network capacity to perform its expected functions [5, 30]. In a WSN, DoS attacks can be classified into following forms [31, 32]:

- Utilization of resource: Since all communication between nodes is done using wireless / radio, they may be easily be targeted.
- Flooding or Devastation of data: It is a technique to send a large number of packets to a single destination. Making overdose of fake message breaks off the wireless communication channels which result noise or collision. In this way the available resource could not be left for legitimate use. These attacks are also known as path-based DoS attacks.
- Physical damage: The DoS attack can exhaust the limited energy and block the communication bandwidth. They can affect the functionality of transceiver by targeting Mac protocols. These attacks can be controlled by carefully running sensor described target.

IV. Existing Approach

A. Swarm Architecture

Swarm intelligence is defined as a study of behavior of biological species such as colonies of ants. In this approach the dynamic behavior of biological spaces is addressed and initialized to make the system intelligent [33] [34]. They are compatible with WSN routing and considered most powerful paradigms of computational intelligence. Various efficient routing techniques can be addressed by the help of SI and WSN.

B. Ant Colony Optimization

It is a met heuristic approach to find out the best path in construction graph. Highly dynamic behavior of ant is utilized to deploy the system. The basic idea of the ant colony optimization (ACO) is searching the food by using the shortest path without directly. Indirect communication between real ants could be made with the help of pheromone. Ants are classified in two categories: In ACO approach ants find out the good quality of food in a good quantity and stored it to their nest. When ants return to their nest they use trail of chemical pheromone, which also guides other ants to reach that particular place where the food source is stored [35]. The working of ACO is shown with the help of flow chart given in Fig. 1.

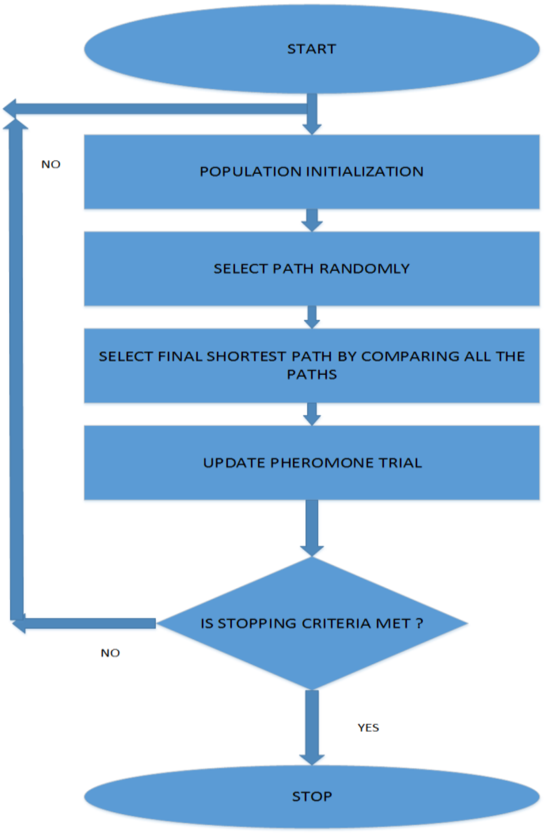
START
POPULATION INITIALIZATION
NO
SELECT PATH RANDOMLY
SELECT FINAL SHORTEST PATH BY COMPARING ALL THE PATHS
UPDATE PHEROMONE TRIAL
IS STOPPING CRITERIA MET ?
NO
YES
STOP

Fig.1. Flow Chart of ACO

V. The Proposed System

In the topology of bait system, a network or bait can be attack in several ways of DoS i.e. Denial of service attacks. The security branch at any ideal agent could affect the whole performance of the application. In the purposed topology the sensors that are idle during routing are termed as "Bait" nodes i.e. upon detecting any intrusion the ideal agent triggers these nodes to have virtual communication with the attacked node and transfer the required information to the main master agent. This virtual communication is dedicated to learn the intrusion.

A. *Architecture of Bait Topology*

Fig. 2 shows that there are three baits and each comprises of many single bait connected with master bait. The main function of master bait is to update the command and control center of any intrusion. The dotted line shows the connection from command and control center to the master in connected bait network. The Command and control center will perform the following functions:

1) Optimal assignment of engagements to specific missile launchers: optimization is understood in terms of probability minimization of a threat successfully attacking the protected area.
2) Commands the best missile launchers to engage the threat.
3) Requests kill assessment to the missile launcher
4) There is an antenna which will transfer the signals from command and control center to the designated missile station for the attack on the intruder

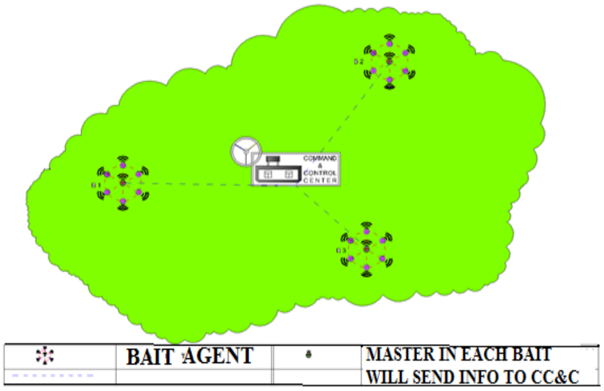

Fig.2. Architecture of Bait Topology

B. *Base Station Monitoring using Bait Agents and the Missile Stations*

Base station is initialized secretly by deploying the group of baits in random manner using UAVs. Fig. 3 shows that the baits B1, B2 etc. are deployed securing inside the base station. These baits have master bait which performs the following functions:

a) Communication with all the bait in its vicinity
b) Update the C & CC (command and control centre)

Each master node in the bait network communicates with all other bait using flooding technique. It is the simplest routing algorithm, which is primarily used when there is no existing knowledge about the network's topology. In the most basic form of flooding, every incoming packet is forwarded to every receiver's neighbor, except the one from which the packet was received. Each node constantly updates its table and sending this information in the form of table to the master node. In this way the master node can get information which node is attacked or stop working. If any node stops working or got tampered the master update this information to the CC & C for necessary action and reshuffle the baits to the new position to recover the distance covered by the attacked node. The Baits in the base station are connected together using Ant colony optimization to recover the Jamming attack by the enemy. If any of the whole bait got jammed the upcoming bait network using ACO can detect this and transmit this information to the CC & C for the necessary action

In a military base station, baits including ideal agents and a master agent are deployed which captures all the activities or data within the real application. The whole performance of bait is measured by quality of data collected and it's processing. Baits main function is to detect an intrusion. The route of sending the information to command and control center needs to be shortest and fastest so that there is no transmission problem at the time of sending information. Command and control center receive the information of all the activities from each bait master agent. The information is processed in command and control Centre and a decision is made whether the activity is normal or terrestrial. This decision is very crucial because a wrong decision can lead to destruction of several lives. If the activity is rejected i.e. the activity is normal no further action is being taken. But if the activity is accepted as a terrestrial activity then all the missile station are alerted by command and control center. On deleting the activity as a terrestrial activity, command centre issues a command to all missile station. The command includes the co-ordinate of the place of activity. All the missile stations get the command and the nearest missile station becomes active and forwards the command to the launcher. On receiving on order from missile station, launcher immediate launches the missile to the given co-ordinates. In this way to place of instruction is destroyed. This is how a base station is secured by a bait system.

VI. Component of Proposed System

Ideal agent/Bait agent: It is the smallest unit of bait system and deployed in monitored area to capture the information from environment to the master ideal agent. In bait, there are many ideal agents who work together and keep rotating in a circular motion to monitor some area and collect sensitive data.

Master agent: In single bait, there is one master ideal agent whose work is to watch the communication link, monitoring the behavior of ideal agent, receives their response and report it to the command and control center.

Command and control center: The bait system has one command and control center which receives the information from master agent. Here, the information is analyzed whether the activity is normal or terrestrial.

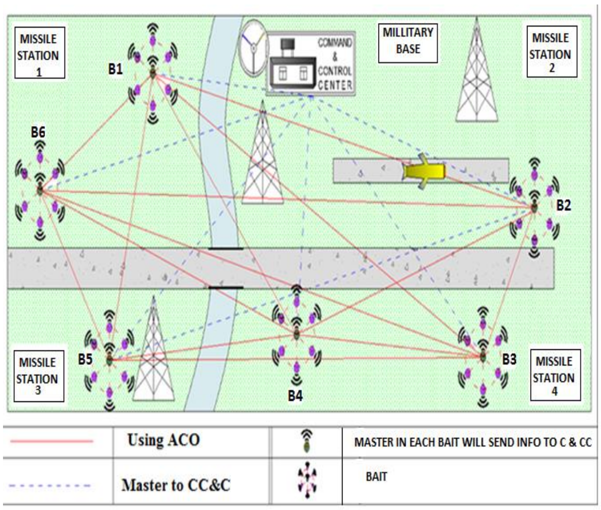

Fig.3. Base Station Monitoring using Bait Agents and the Missile Stations

Command Centre sends the information to missile station if the activity is found to be unsatisfactory. Moreover, command and control center can control the ideal agent in bait to deal witch some special event as gamming attacks.

Missile station: It receives the command from command and control center. The co-ordinates of destination for launching the missile are given by control center. If the missile station is nearest to the destination it will activate and launch the missile.

Bait Network: In bait network there are many ideal agents which are connected to a single master agent. Bait agent rotate in a circular manner to detect any activity in their area. Every bait agent has its particular area and reports all the activities to its master agent.

Missile station: There are many missile station developed at military base station are directly connected to control center, missile stations receives the command from control center in which co ordinations of place are given. The missile station

VII. Architecture of Intrusion Detectionsystem

The main aim of this architecture is to overcome the different DoS attacks in physical layer like

a) *Tampering* – where only the monitoring node (Bait) got jammed or got affected.
b) *Jamming* - where a group of bait node with the master node got jammed or got affected.

In a base station many types of bait are deployed in random manner using UAVs. A bait network comprises of many Bait agent and from those agent, one agent acts as a master agent. The Bait agent in a Bait network rotates in a circular motion and monitors their respective area in order to collect sensitive data. If any intrusion is found by any bait agent update master agent using flooding and master agent forwards the information to command and control center. Which is near to the place becomes active and issues an order to the launch missile.

A. Tampering

In Tampering, an intruder may enter in the area of a particular agent and try to capture the information. If any Bait “X” has been attacked by the enemy in any of the bait network then it will get disconnected from the bait network. Since every other nodes maintains a global table of other nodes connection in that bait network, and this table is updated and flooded to all other nodes in the network at regular interval by PING and ACK signals. The Bait “X” will not reply ACK to other nodes, so every node will update the table that “X” bait is not reachable when the local master will also not get the ACK from Bait “X”, so it will check the table of other nodes table for the connectivity of bait “X”. If in those table it was shown that Bait “X” is not reachable then it will automatically inform the master node and master node will automatically updates this information to CC & C for necessary action. An example of such system is shown in Fig. 4.

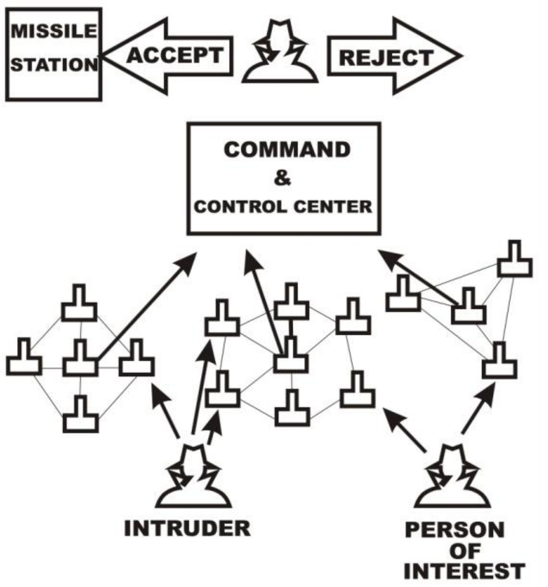

Fig.4. Bait Network Showing the Tampering case B. Jamming

An intrusion may come and may join the whole bait in order to enter safely into military base. In this situation, the master ideal agent can't send the information to command and control center, this situation is known as Jamming.

To overcome this type of problem the connected master agents of other Bait network immediately inform the command center. The entire master ideal agent will be connected with each other to share the information also all Baits change their position from one place to another using Ant Colony optimization. If all Bait networks deployed in the base station got jammed then at least we can track the route followed by the bait networks for future use. Fig. 5 depicts a jamming network.

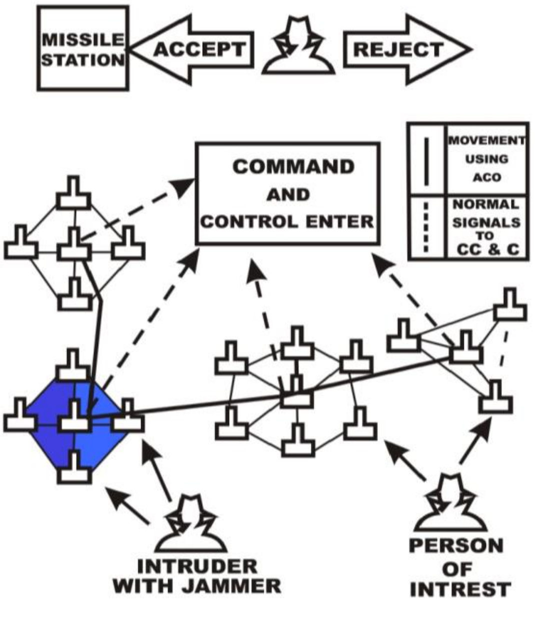

Fig.5. Bait Network Showing the Jamming Case

In both types of instruction, when Bait sends the information to the command and control center, it fuses the information and decides that the activity is normal or terrestrial. If the activity is found to be terrestrial, command and control Centre sends this information to the missile station. Command and control center is connected to all the master ideal agent of all the Baits and missile station. On receiving the command from the control center, the Missile station launches the missile to that place where terrestrial activity is found. In this way, Bait system works in the Military base.

VIII. Conclusion

The development of sensor technology is an essential part of modern military applications. Deploying these sensors especially in remote environment in a successful manner is a crucial task. In this paper a new model of security and monitoring applications is proposed which is based on "Bait" system. The baits include ideal agents and master agents. These agents capture information from the activities detected within the range and send the same to the control system. The whole system uses a simple routing algorithm for information exchange. The bait system, master agents along with the command control centre make the whole system secure and active. The proposed system is fast, secure and feasible to install in military based applications.

References

[1] R. Muraleedharan and L. A. Osadciw, "An Intrusion Detection Framework for Sensor Networks Using Honeypot and Swarm Intelligence," 6th Annual International Conf. on Mobile and Ubiquitous Systems: Computing, Networking and Services, Toronto, pp. 1-2, 13-16, July 2009.

[2] I. Melgar, J. Fombellida, J. Seijas and F.Quintana, "Cooperation and competition based on Free Market in Swarm System architectures for Air Defense," IECON 09, pp. 3359-3364, November 2009.

[3] Rajani Muraleedharan and Lisa Ann Osadciw, "An Intrusion Detection framework for Sensor Networks using Ant Colony," ACSSC 2009, Pacific Grove, pp. 275-278, 1-4 Nov. 2009.

[4] M. Jamshidi, *Systems of Systems Engineering: Principles and Applications*, CRC Press, FL USA 2008.

[5] Wood A.D., Stankovic. J. A., "Denial of Service in Sensor Networks," IEEE Computer, vol. 35, Issue: 10, Oct. 2002.

[6] Y. M. Yussoff, H. Hashim, R. Rosli, and M. Dani Baba, "A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks," International Symposium on Robotics and Intelligent Sensors, vol. 41, Issue. 4, pp. 580-587, April 2012.

[7] Medium Extended Air Defense System (MEADS) 21st Century Air and Missile Defense, 2008.

[8] Vijayasarathy, R., Ravindran, B., and Raghavan, S.V., "A system approach to network modeling for DoS detection Using a Naive Bayesian classifier," IEEE COMSNETS, 2011, Bangalore, pp. 1-10, Jan. 2011.

[9] X. Ouyang, B. Tian, Q. Li, J. Zhang, Z. Hu, and Y. Xin, "A Novel Framework of Defense System Against DoS Attacks in Wireless Sensor Networks," WICOM 2007, Wuhan, pp. 1-5, Sept. 2011.

[10] A. D. Wood, John A. Stankovic, and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks,"

Proceedings of the 24th IEEE International Real-Time Systems Symposium, 2003, pp. 286-297.

[11] A. Mittal, A. K. Shrivastava, and M. Manoria, “A Review of DDoS Attack and its Countermeasures in TCP Based Networks,” International Journal of Computer Science & Engineering Survey (IJCSES) vol. 2, no. 4, pp. 178-187, November 2011.

[12] H. Beitollahi and G. Deconinck, “Tackling Application-layer DDoS Attacks,” Procedia Computer Science, vol. 10, pp. 432-441, 2012.

[13] H. Chen, T. Gaska, Yu Chen, and D. H. Summerville, “An optimized reconfigurable power spectral density converter for real-time shrew DDoS attacks detection,” Computers and Electrical Engineering, vol. 39, pp. 295-308, 2013.

[14] M. Aamir and M. A. Zaidi, “DDoS Attack and Defense: Review of Some Traditional and Current Techniques,” Interdisciplinary Information Sciences, vol. 19, no. 2, pp. 173–200, 2013.

[15] M. J. Hashmi, M. Saxena, and R. Saini, “Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System,” International Journal of Computer Science & Communication Networks, vol. 2, no. 5, pp. 607-614, 2012.

[16] M. H. Bhuyan, D.K. Bhattacharyya, and J. K. Kalita, “An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection,” Pattern Recognition Letters, vol. 51, pp.1-7, 2015.

[17] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, “A game theoretic defence framework against DoS/DDoS cyber-attacks,” Cryptography Group, Faculty of Engineering, University of Bristol, Merchant Ventures Building, Woodland Road, Clifton BS8 1UB, UK.

[18] Wei Zhou, Weijia Jia, Sheng Wen, Yang Xiang and Wanlei Zhou, “Detection and defense of application-layer DDoS attacks in backbone web traffic,” Future generation Computer System, vol. 38, pp. 36-46, September 2014.

[19] T. Thenmozhi and R.M. Soma, “Towards an approach for improved security in Wireless Sensor Networks,” ICCCNT’ 12, Coimbtore, India, pp. 26 -28, July 2012.

[20] D. J. Thuente and M. Acharya, “Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks,” in Proceedings of Military Communications Conf. Atlantic City, USA, (MILCOM), 2006.

[21] W. Xu et al., “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” Proc. 11th Ann. Int’l Conf. Mobile Computing and Networking, ACM Press, pp. 46–57, 2005.

[22] T. Kavitha and D. Sridharan, “Security vulnerabilities in wireless sensor networks: a survey,” Journal of Information Assurance & Security, vol. 5, pp. 31-44, 2010.

[23] D. Raymond et al., “Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols,” *Proc. 7th Ann. IEEE Systems, Man, and Cybernetics Information Assurance Workshop*, IEEE Press, pp. 297-304, 2006.

[24] Padmavathi and G. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” International Journal of Computer Science and Information Security (IJCSIS): vol. 4, no.1 & 2, Dec. 2009.

[25] Karlof. C and Wagner. D, “Secure routing in wireless sensor networks: Attacks and countermeasures,” In Proc. of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, May 11, 2003.

[26] E. L. Caballero, “Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks-The routing problem,” TKK T-110.5290, Seminar on Network Security, 2006.

[27] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless Sensor Network Security: A survey,” Security in distributed, grid, and pervasive computing, Auer Bach Publications, CRC Press, ISBN 0-849-37921-0, 2006.

[28] T. Petrović and M. Žagar, “Security in Distributed Wireless Sensor Networks,” In Proc. of the 35th International Convention MIPRO, Croatia, May 2012.

[29] Y. Zhou, Y. Fang and, Y. Zhang, “Securing Wireless Sensor Networks: A Survey,” IEEE Communications Surveys & Tutorials,” vol. 10, issue 3, pp. 6-28, 2008.

[30] A. Abduvaliyev, Al-Sakib K. Pathan, J. Zhou, R. Roman and, W. C. Wong, “On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks,” IEEE Communication Surveys and Tutorials, July 2013.

[31] ZHANG Yi-ying, LI Xiang-zhen and, LIU Yuan-an, “The detection and defence of DoS attack for wireless sensor network,” The Journal of China Universities of Post and Telecommunication, pp. 52-56, Oct. 2012.

[32] M. Sharawi, I. A. Saroit, H. Mahdy, and E. Emary, “Routing Wireless Sensor Networks Based On Soft Computing Paradigms: Survey,” International Journal on Soft Computing, Artificial Intelligence and Applications (IJSCAI), vol. 2, no. 4, August 2013.

[33] Z. Ali and W. Shahzad, “Analysis of Routing Protocols in AD HOC and Sensor Wireless Networks Based on Swarm Intelligence,” International Journal of Networks and Communications, vol. 3, no. 1, pp. 1-11, 2013.

[34] S. U. Parvatkar and D.V. Gore, “An Ant Colony Optimization Algorithm for maximizing the lifetime of Heterogeneous Wireless Sensor Network,” International Journal of Current Engineering and Technology, vol. 4, no. 3, June 2014.

Authors’ Profiles

Abdus Samad Completed his B.Sc. Engg. (B. Tech.) and M. Tech. from Z.H. College of Engineering & Technology, Aligarh Muslim University (AMU), Aligarh, India in the year 1997 and 1999 respectively. He has completed his Ph.D in Computer Engg. from Dept. of Computer Engg., AMU in the year 2010. The current research areas are Parallel and Distributed Systems, Microprocessor and Embedded System Design.

He has contributed and attended various national and international conferences in India and abroad. He has published various research papers in reputed journals. He is a member of IETE and associated himself with other Universities for academic interest.

Dr. Samad presently working as Associate Professor in Computer Engineering at University Women’s Polytechnic, AMU, Aligarh and having teaching experience of more than 19 years. Besides academic, he is also sharing various other responsibilities of examinations and administrations in the department. He actively participated in various positions in University administration.

Mohammed Shuaib is presently working as a lecturer at Department of Computer Science, Jazan University, KSA. His Research area is Security, Artificial intelligence, Sensor network, Cloud Computing and Intrusion Detection Techniques. He received his M. Tech in Software Engineering from Department of Computer Engg., AMU, Aligarh, India in the year 2012. He has also served for three years as an Assistant Professor in the Department of Computer Engg., Integral University, Lucknow, India.

Mohd Rizwan Beg is working as a Professor and Director of RBGI group, Agra. His areas of expertise are Software Engg., Requirement Engineering, Data Mining, Software Quality, and Software Project Management. He has delivered expert lectures and contributed in various national and international conferences in India and abroad. He has published more than 40 papers in reputed journals and conferences. Presently 8 research scholars are pursuing their Ph. D in his supervision.

He is Associate Editor in Chief of Advancement in Computing Technology & is also member of editorial board for various other International & National Journals. He is member of large member of International professional societies & also member of Advisory Board for various institutions in India. He chaired a number of workshops, seminars & conference.

Prof. Beg has served for many years as a Head in Department of IT, Integral University, Lucknow, India. He was having various responsibilities at Integral University like Controller of Examination and discharge other administrative responsibilities within and outside department. He is having teaching experience of more than 25 years.

How to cite this paper: Abdus Samad, Mohammed Shuaib, Mohd Rizwan Beg,"Monitoring of Military Base Station using Flooding and ACO Technique: An Efficient Approach", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.12, pp.36-44, 2017.DOI: 10.5815/ijcnis.2017.12.05