International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 8, Issue 5, May 2020||

Location Aware Data Sharing and Attack Revocation on End to End Secure Routing in WSN

P.Sathishkumar[1], Nivetha SR[2]

Associate Professor, Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Tiruchengode, Tamilnadu, India[1]

B.E Student, Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Tiruchengode, Tamilnadu, India[2]

ABSTRACT: The main trouble of clustering approaches for wireless sensor networks (WSNs) is to prolong the battery lifetime of the individual sensors and the network lifetime. In this paper we put forward a homogeneous and secure weighted clustering algorithm which is an extended version of our previous algorithm with a combination of 5 metrics. Among these five metrics the behavioral level metric which promotes a secure choice of a cluster head within the sense where the last one will never be a malicious node. Previous approaches have focused on the formalization of attack graphs into a Bayesian model instead of proposing mechanisms for his or her analysis. In this paper we propose to use efficient algorithms Cluster Based Bayesian Attack Monitoring System (CBAT) to make exact inference in Bayesian attack graphs, enabling the static and dynamic network risk assessments. To strengthen the validity of our approach we executed an experimental evaluation on synthetic Bayesian attack graphs with different topologies, showing the computational advantages in terms of time and memory use of the proposed techniques in comparison with existing approaches.The goal of the proposed algorithm is to offer a better performance in terms of the quantity of re-affiliations which enables to urge a reduced number of balanced and homogeneous clusters. This algorithm, including suitable routing protocols, aims to take care of stable clustering structure. We use simulation study to reveal the performance of the proposed algorithm.

I.INTRODUCTION

1.1 Wireless Sensor Networks

A WSN (Wireless Sensor Network) consists of a large number of sensors, each of which are physically small devices, and are equipped with the capability of sensing the physical environment, data processing, and communicating wirelessly with other sensors. Generally, we assume that each sensor in a WSN has certain constraints with respect to its energy source, power, memory, and computational capabilities.

The communication paradigm of WSN has its root in wireless ad hoc networks, where network nodes self-organize in an ad hoc fashion, usually on a temporary basis.In a wireless ad hoc network, a group of wireless nodes spontaneously form a network without any fixed and centralized infrastructure. When two nodes wish to communicate, intermediate nodes are called upon to forward packets and to form a multi-hop wireless route.

A new wireless sensor network consists of individual sensor nodes which measure various environmental variables. Most of the variables depend on the application and can range from physical parameters, such as temperature or humidity, to more abstract parameters. This information can be stored as data at the node or relayed through the network, using wireless communications, for access by the user. It is used to measure distance between the nodes.

1.2 Unique Characteristics of Wireless Sensor Networks

The number of the nodes in a sensor network is significantly larger than that in a typical wireless ad hoc network. The difference is often of several orders of magnitude. Sensors are usually low-cost devices with severe constraints with reference to energy source, power, computation capabilities and memory. Sensors are usually densely deployed.

1.3 Application Wireless Sensor Network

Development of WSNs was primarily motivated by their need for military surveillance. With the availability of low-cost sensors, these networks are no longer limited to military applications but are used in a wide array of applications including habitat monitoring, industrial process monitoring, traffic control, etc

1.3.1 Military Application

Military missions often call for high risk to human personnel. Thus, unmanned surveillance missions using WSN have wide applications for military purposes such as surveillance, enquiry of opposing forces, targeting, damage assessment, etc. WSNs developed for military purposes should be rapidly deployed in an ad-hoc fashion such as by an aircraft.

1.3.2 Habitat Monitoring

Monitoring plant and animal habitats on a long-term basis is widely employed by researchers in Life Sciences. However, human presence in such monitoring often causes disturbances in plant and animal conditions, increases stress, reduces breeding successes, etc. WSNs provide a non-invasive and economical method of long-term monitoring of habitats. Such a network was used to monitor the Storm Petrel seabirds in the Great Duck Island in Maine. Wireless sensors were used to measure temperature, pressure, humidity was used to track zebra and other animals in Kenya.

1.3.3 Environmental Monitoring

WSN can be used in a wide range of environmental monitoring applications such as forest fire monitoring, air pollution monitoring, greenhouse gas monitoring etc. WSNs to monitor dangerous gases such as CO, NO2, and CH4 have already been deployed in some cities.

1.3.4 Agricultural Monitoring

Wireless sensors may be deployed across large areas of crop fields and can monitor different parameters like moisture and fertilizer content of soil, temperature this can automate the processes of irrigation application of fertilizer and pesticides, among others, minimizing human intervention and maximizing yield.

1.3.5 Industrial Monitoring

Industrial machineries need condition-based maintenance. Wired infrastructure for such maintenance is costly due to the cost of wiring and the inaccessible locations, such as rotating machinery. Wireless sensors are beneficial insuch cases, providing greater accessibility, improved monitoring and maintenance at lower costs.

1.3.6 Health Monitoring

Wireless personal area or body networks may revolutionize the way we monitor health conditions by providing a non-invasive, inexpensive, continuous and ambulatory health monitoring. Patients wear small body sensors that monitor the patient's bio-signals such as heart rate, and the collected data are transmitted over a hand held device. Alarms and bio-signals may be transmitted over the Internet to a health professional for real-time diagnosis.

1.4 Challenges in Wireless Sensor Network

Some of the major challenges that prevent the wide spread adoption of WSNs are listed below

1.4.1 Energy Constraint

Wireless sensor nodes are battery-powered and often deployed in remote and inhospitable locations. As such, battery replacement or any other human intervention is either not possible or extremely difficult. Therefore, these nodes are required to function for months or years at a time on the same power source to maintain the application Quality of Service (QoS). As a result, energy conservation is of the utmost importance in WSNs, and much research has been done on the development of energy efficient protocols and hardware for WSNs.

1.4.2 Fault Tolerance

Often a sensor node may be destroyed or stop functioning, such as when a sensor node is destroyed in a forest fire or by the enemy in a battlefield. The remaining nodes must adapt dynamically in real time and convey the data to the base stations or sinks. Thus, WSN protocols for the MAC and routing layers must have a certain level of robustness.

1.4.3 Computational Capability

Sensor nodes are small devices with very limited memory and processing power. Thus, often at times large scale processing is not possible in sensor nodes, and the data must be transmitted to a base station to be processed. However, with the advancement of semiconductor technology, this drawback has been greatly reduced.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 8, Issue 5, May 2020||

1.4.4 Security

WSNs are lightweight networks with limits on the transmitting data rate and capacity. Thus, conventional security measures such as private keys are not readily applicable to such networks, as these may increase the network overhead and in turn decrease the network lifetime. However, security is an important requirement in applications such as surveillance. Thus, another area of research in WSNs is providing security and privacy.

1.5 Working of WSNs

WSN mechanism is quite easy, simple and applicable to a variety of fields. The system is totally reliant on the nodes and the harmony established between them through proper frequency. These nodes are of different sizes according to the function they perform.

To operate the monitoring or tracking function of these nodes a radio transmitter is attached to forward the information signals in the form of waves. They are controlled by the microcontroller according to the function and device in which they are used.

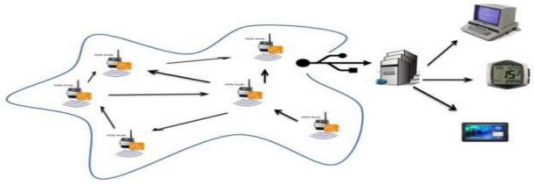

Fig.1 WORKING OF WSN

The WSNs perform function concurrently where nodes are autonomous bodies incorporated in the field spatially for the accurate results. The information transmits through proper channel taking the knowledge collecting it within the sort of data and send to the bottom.

Depending to their types WSNs are used by different organizations and fields to monitor a specific task. WSN are incorporated at different point to monitor a specific area a commonly known example is that of military communication either land or water. Major issues which are getting a possible threat to life are environmental and industrial issues. WSNs are doing great job in the relevant fields to sense to temperature for greenhouse gasses and similarly earthquake detectors are implanted to detect the land sliding phenomenon for precautionary measurements etc.

1.6 Inference Monitoring in WSN

A wireless sensor network (WSN) is a large ollection of densely deployed, spatially distributed, autonomous devices (or nodes) that communicate via wireless and cooperatively monitor physical or environmental conditions.

In such network, sensor nodes are deployed over a geographic area (called the region of interest or ROI) by aerial scattering or other means. Each sensor node can only recognize events within some very limited distance from itself called the sensing range. In addition, sensor nodes normally have fairly limited transmission and reception capabilities in order that sensing data need to be relayed via a multi-hop path to a foreign base station (BS), which may be a data collection center with sufficiently powerful processing capabilities and resources.

Various reasons such as battery exhaustion and physical destructions by attackers. They may also be moved away from where they were deployed by animals, winds, or other environmental means. As a consequence of node failures, node movements and other unpredictable factors, the topology may change with time. It is, therefore, critical that the BS learn in real time how well the WSN performs the given sensing task under dynamically changing network topology.

We define the gathering of of these positions within the ROI because the connected coverage (or coverage in short). Obviously, it's one among the foremost important performance metric measuring the standard of surveillance a WSN can provide. The BS also should have the power to watch the coverage status in real time. Although much research has been conducted to ensure high network coverage and connectivity. Possible causes resulting in coverage holes include energy depletion of sensor nodes, intended attacks on sensor nodes, and so on. In many WSN applications, especially security-sensitive applications, it's a requirement to accurately detect the coverage boundary. The protocol developed during this paper can affirmatively answer this open challenging issue. On the opposite hand, problems associated with the self-monitoring of a WSN are studied within the literature for various applications and purposes. For example, Chessa and Santi [30] propose one time-out scheme to watch the system-level fault diagnosis. A residual energy scan is meant to approximately depict the remaining energy distribution within a WSN.

However, of these schemes can't be directly used for the coverage inference, as they're either centralized schemes or assume that every individual sensor within the WSN must be monitored. This is not true for our case because the BS only must make sure that a ceratin percentage of the sensors are functioning, especially when the WSN is densely deployed.

II. EXISTING SYSTEM

In existing system is decisive and allows the energy and bandwidth management clustering algorithm to avoid any malicious node in the neighborhood to become a CH, even if the remaining metrics are in its favor. The election of fixed CHs is carried out using weights of neighboring nodes which are computed based on selected metrics. So, this strategy ensures the election of legitimate CHs with high weights. The preliminary results obtained demonstrate the effectiveness of our algorithm and in terms of the amount of equilibrate clusters and therefore the number of reaffiliations, compared to WCA (Weighted Clustering Algorithm), DWCA (Distributed Weighted Clustering Algorithm), and SDCA (Secure Distributed Clustering Algorithm). These results also reveal that our approach is suitable if we decide to use it in network layer reactive routing protocols rather than proactive ones once the clustering mechanism is launched.

2.1 Drawbacks of Existing System

- Fixed cluster head cannot manage bandwidth levels all the time.
- Low data and energy management.
- No proper maintaining stable clustering structure and offering a better performance.
- Not showing clearly the interest of the routing protocols in energy saving and therefore maximizing the lifetime of the global network.
- Poor performance.

III.PROPOSED SYSTEM

(C-BAT) is adapted from the conventional Routing Information Protocol (RIP) to ad hoc networks routing. It adds a replacement attribute, sequence number, to every route table entry of the traditional RIP. The newly added sequence number, the mobile nodes can diferentiate state route information from the new and thus prevent the formation of routing loops.

Packet Routing and Routing Table Management in C-BAT, each mobile node of an ad hoc network maintains a routing table, which lists all available destinations, the metric and next hop to every destination and a sequence number generated by the destination node. Using such routing table stored in each mobile node, the packets are transmitted between the nodes of a network.

Each node of the unplanned network updates the routing table with advertisement periodically or when significant new information is out there to take care of the consistency of the routing table with the dynamically changing topology of the unplanned network.

This indicates that every receiving neighbor is one metric (hop) far away from the node. It is different from that of the conventional routing algorithms. After receiving the update packet, the neighbors update their routing table with gain of metric by one and retransmit the update packet to the corresponding neighbors of every of them.

The process is going to be repeated until all the nodes within the unplanned network have received a replica of the update packet with a corresponding metric. The update data is additionally kept for a short time to attend for the arrival of the simplest route for every particular destination node in each node before updating its routing table and retransmitting the update packet.

If a node receives multiple update packets for a same destination during the waiting period of time, the routes with newer sequence numbers are always preferred because the basis for packet forwarding decisions, but the routing information isn't necessarily advertised immediately, if only the sequence numbers are changed. If the update packets have an equivalent sequence number with an equivalent node, the update packet with the littlest metric are going to be used and therefore the existing route are going to be discarded or stored as a less preferable route. In this case, the update packet is going to be propagated with the sequence number to all or any mobile nodes within the unplanned network.

The elements within the routing table of every mobile node change dynamically to stay consistency with dynamically changing topology of a billboard hoc network. To reach this consistency, the routing information advertisement must be frequent or quick enough to make sure that every mobile node can nearly always locate all the opposite mobile nodes in the

dynamic ad hoc network. Upon the updated routing information, each node has got to relay data packet to other nodes upon request within the dynamically created unplanned network.

3.1 C-BAT (Extended version of weighted Clustering Algorithm with C-BAT Routing)

The Proposed Homogeneous Clustering Algorithm the stress of our approach is to extend the lifetime of the network by ensuring a homogeneous distribution of nodes within the clusters so that there's not an excessive amount of receiving and transmitting overhead on a Cluster Head.

DSR with C-BAT Basic assumption for the clustering algorithm

- the bottom station (BS) is found far away from the sensors and immobile.
- All nodes within the network are homogenous and energy-constrained.
- All nodes are able to send data to BS.
- The BS has the knowledge about the situation of every node.
- At the beginning energy of all nodes is at the utmost level.
- within the first round, each node features a probability p of becoming the cluster head.
- Nodes within the network aren't dynamic while the Cluster Heads (CHs) are being.

3.2 Proposed Algorithm

Step#1: within the first round, BS collects information regarding location of all the nodes within the network. Depending on the density and geographical layout of the network, it virtually divides the network into 10 zones. The objective behind this method is to make sure uniform selection of CHs throughout the layout of the network.

Step#2: Since we have assumed that initially all the nodes have same maximum energy (Emax), the nodes in each zone have a probability p (1/number of nodes in the zone) of becoming a CH. Hence, from each zone, randomly a cluster head (CH) is chosen randomly.

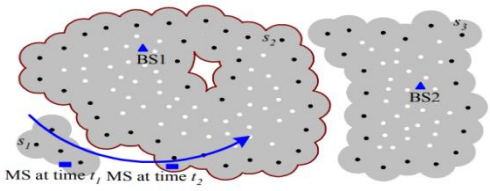

Fig.2 Joining Request of Nodes

Step#3: Once the CHs are formed, it broadcasts its identity to all or any the opposite nodes within the network to simply accept it joining request and form actual clusters. For example, CH7 and CH12 broadcast its identity to all or any the nodes within the network.

Step#4: The nodes which accept the joining request analyses the signal strength. Signal strength of the CH request depends on the space between CH and node.

Step#5: The CH prepares the info sending schedule and sends it to its members within the cluster.

Step#6: The CH receives data from each node, compresses the info and sends it to the BS.

IV.MODULES

4.1 Request Cluster head Scheduling Model

In this module to maintain ultimate goal of CH energy is to schedule data accessing requests so that the total energy consumption is minimized, while all requests are transmitted within their constraints. The problem can be modeled as follows. Consider a sequence of n requests, which comprise the four previously defined categories of requests. When the transmission is completed and no additional transmission occurs, the state machine remains in the high-power state for configured time units before transiting to intermediate-power state.

If no transmission occurs, the state machine remains in the intermediate-power state for observed time units before transiting to the lower-power state, where T1 and T2 are the tail time. Even when multiple requests are simultaneously

transmitted, state transition remains the same with only one request. This action not only uses the tail time, but also reduces TRM and various promotions.

Fig.3 Reputation Manager Details

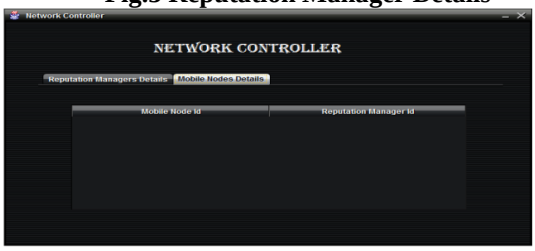

Fig.4 Mobile Node Details

4.2 C-BAT Energy Consumption Model

In this module to construct an accurate energy model, conduct a series of measurements on the thing Energy Profiler to get a group of energy consumption data. supported the info set, analyze the energy consumption of various states and state transitions. where a transmission process refers to the change in power state from low to high then back to low.

To identify the parameters of our energy model, we conduct two measurement experiments. We build an internet server with configurable bandwidth, and energy consumption is measured when the phone downloads a file from the online server under different bandwidth configurations. Next a message receiver is started on the phone. Then send messages to the phone from another device and keep the state machine within the minimum state while energy consumption is measured.

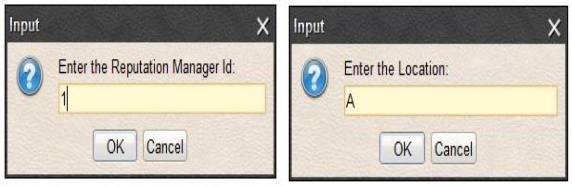

Fig.5 Input of Manager Id and Location

4.3 Random Cluster Noding

In this module to distinguish different requests defined by applications, Random cluster provides a customized API for such applications. An application informs Random cluster how to process a request via a simple API Submit Request (r _ delay).

If r_ delay is 0, the request may be a real-time or an unsuccessfully prefetched request (successfully perfected request would not be submitted) that should be transmitted instantaneously.

If r_ delay is a positive value, the request is delay-tolerant and be delayed for r_ delay time units.

If r_ delay is a negative value, the request is a previous attempt that likewise can be delayed for -r_ delay time units.

However, the difference between delay-tolerant request and former attempt is that the latter would be discarded because the deadline approaches. Random cluster schedules requests as indicated by the parameter r_ delay.

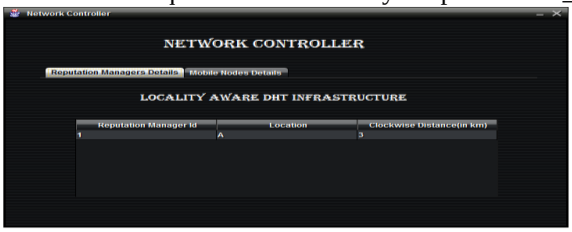

Fig.6 Measured time Delay of Nodes

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 8, Issue 5, May 2020||

4.4 Data Transmission and Verification

In this module two tail times can be directly applied to one tail time. Thus, we consider only the former. We separate the 2 tail times primarily because the scheduling rates in these two periods are distinct. Two mechanisms are employed for online determination of whether now's the tail time.

Power-based state inference mechanism is employed to infer the present RRC state supported power consumption. Determining the present RRC state is that the foundation of distinguishing between the 2 sorts of tail time.

Virtual tail time that is used to determine whether now is the tail time, which corresponds to the original inactivity timers maintained by the RNC. After transmitting data within the tail time, the inactivity timers are reset, such the physical tail time is broken. We ask the used tail time because the virtual tail time.

A timer is required to work out whether now's the virtual tail time within the current RRC state. The virtual tail timer, performs operations that are similar to those performed by the inactivity timer maintained by the RNC. Two timers correspond to the virtual tail times of the DCH and ACK states, which are denoted as γ and δ, respectively.

Similar to the inactivity timer α, the virtual tail timer γ is activated when the throughput is 0 or under the configured threshold.

1.If timer γ is activated when the throughput is 0, Random cluster can start transmitting data after the timer γ is activated and stop when the timer γ expires or is reset.

2.If timer γ is activated when the throughput is under the configured threshold but greater than 0, Random cluster cannot transmit data after the timer γ is activated.

If Random cluster transmits data under this condition, the transmission of real-time data may be ongoing when the timer γ expires, and demotion at this time would trigger additional state promotions. Thus, having no transmission at the second condition would not reset the inactivity timer α, and the state is demoted to the ACK state after the expiry of timer α. When in the ACK state, the virtual tail timer δ would be activated only when the throughput is 0. Random cluster can start transmitting data after timer δ is activated and stop when the timer δ expires or is reset.

Fig.7 Data Transmission Successful

4.5 Data Queuing Management

In this module to handle the scheduling requests feasibly, is another problem to be discussed in this section. Applications submit CH requests by calling the API. Requests that can be delayed, referred to as Random cluster requests, include delay-tolerant requests and previous attempts. Random cluster employs a dual queue scheduling algorithm for scheduling these two categories of requests.

Random cluster schedules requests by maintaining two queues:

1.Real-time queue for requests that must be scheduled instantaneously, and

2.Random cluster queue for Random cluster requests.

Random cluster schedules requests in the real-time queue if requests are present in this queue and schedules those in the Random cluster queue if the real-time queue is empty or if the deadline of the first request in the Random cluster queue approaches.

Fig.8 Queue Management

4.6 Handling Random Cluster Requests

Random cluster is feasible if and only if it not only transmits requests in the real-time queue as soon as they are inserted, but also processes requests in the Random cluster queue before their deadlines. Specifically, delay-tolerant requests should be scheduled before their deadlines, and former attempts should be scheduled before their deadlines or discarded as their deadlines approach.

After being delivered by applications, Random cluster requests are added to the queue from small to large, according to the time between tnow and di, where tnow is the current time, and di equals to the sum of the arrival time ai and the absolute value of r_delay of request i. The first request in the Random cluster queue is assigned with the latest deadline and is the first to be transmitted.

After each enqueue operation, Random cluster derives the latest deadline, denoted as dl, and restarts the timer θ, the end time of which is dl −tnow. When now's the virtual tail time, the primary request within the queue is dequeued first. Timer θ is canceled before the first request is dequeued and reactivated according to the deadline of the next request in the queue after dequeuing.

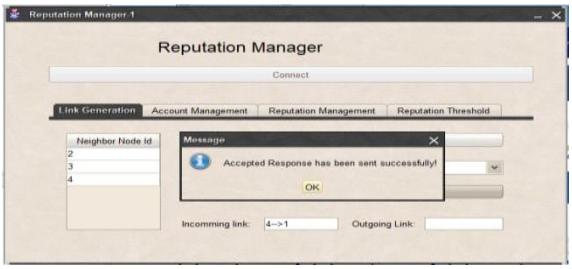

Fig.9 Accepted Responses of Nodes

4.7 Transmission Controlling Mode

In the virtual tail time of the ACK state, excessively high transmission speed expands the occupancy of the RLC buffer to a level greater than the threshold set by the RNC. This expansion results in ACK→DCH promotion, thereby causing additional energy consumption. To prevent triggering promotions when transmitting requests in the ACK state, Random cluster transmits data according to the size and consumption time of the RLC buffer, and ensures that the buffer occupancy level does not exceed the threshold. Let bot denote the buffer occupancy in the current time and BO denote the buffer occupancy threshold set by the RNC. Request scheduling of Random cluster in the virtual tail time of the ACK state should satisfy the state.

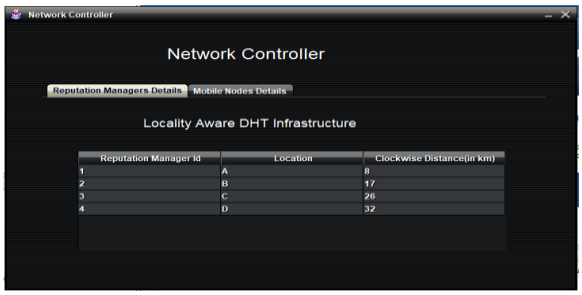

Fig.10 Output of the Manager Id and Nodes

V.CONCLUSION

In this work, we proposed a new algorithm called "MACWWSN " is proposed for the specificities and constraints of sensor networks. Using MACWWSN we aimed at creating a virtual topology to minimize frequent re-election and avoid overall restructuring of the entire network. Our first objective is to reduce energy consumption in all levels. As a result of this work, we plan to exploit the concept of redundancy to enhance results that are related to energy conservation. Another interesting work that remains to do is to provide in-network processing by aggregating correlated data in the routing protocol and reduces the amount of data that are transported in the network.We have further shown the importance of modelling AGs taking into account the subnetwork structure of typical corporate networks. Network clustering enables the dynamic analysis with the C-BAT algorithm to become tractable and scales linearly in the number of nodes. This allows to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 8, Issue 5, May 2020||

rapidly integrate new evidence in the analysis and enables administrators to respond to an ongoing attack. Further this include exploring more scalable inference techniques, extending the BAG model to form it less restrictive, and investigating more accurate means of estimating the probability of exploitation of vulnerabilities.

REFERENCES

[1] Alan D. Amis, Ravi Prakash, Thai H.P., Vuong Dung, T. Huynh. Max-Min D-Cluster Formation in Wireless AdHoc Networks. Proceedings of IEEE conference INFOCOM 2010.

[2] A.Boukerche,Algorithms and Protocols for Wireless Sensor Networks. Wiley-IEEE Press, 2008

[3] BenjieChen,KyleJamieson,HariBalakrishnan,RobertMorris.Span:AnEnergy Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc WirelessNetworks.Wireless Networks 8, 481–494, 2002, Kluwer Academic Publishers.

[4] E. F. Nakamura, A.A.F. Loureiro, and A.C. Frery, "Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications," ACM Computing Surveys, vol. 39, no. 3, pp. 9-1/9-55, 20012.

[5] Haowen Chan, Adrian Perrig. ACE: An Emergent Algorithm for Highly Uniform Cluster Formation. Proceedings of the First European Workshop on Sensor Networks (EWSN), Vol. 2920 Springer (2004) , p. 154- 171.

[6] Maniakchatterjee, Sajal. K.das, DamlaTurgut. WCA: A Weighted Clustering Algorithm for wireless adhoc networks. Journal of cluster computing (Special issue on Mobile AdHoc Networks) 2012.

[7] Mao Ye1, Chengfa Li, Guihai Chen1, Jie Wu. EECS: An Energy Efficient Clustering Scheme in Wireless Sensor Networks. 24th IEEE International Performance, Computing, and Communications Conference, 2009. IPCCC 2009.

[8] V. Loscrì, G. Morabito, S. Marano.: A Two-Levels Hierarchy for Low-Energy Adaptive Clustering Hierarchy (TL-LEACH). Proceedings of IEEE 2005, 0-7803-9152-7/05.

[9] P. Kumarawadu, D. J. Dechene, M. Luccini, A. Sauer. Algorithms for Node Clustering in Wireless Sensor Networks: A Survey. Proceedings of IEEE 2008.

[10] Wu Xinhua, Wang Sheng. Performance Comparison of LEACH & LEACH-C Protocols by NS2. 9th International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010.