Secured Redundancy Mechanism to Detect Intrusion in Heterogeneous Wireless Sensor Networks

Sudarshan T V
Department of computer science and Engg.
Akshaya Institute of Technology
Tumkur, India

Manjesh B N
Department of computer science and Engg.
Akshaya Institute of Technology
Tumkur, India

***Abstract*— The previous few years have seen an enlarged interest in the prospective utilize of wireless sensor networks (WSNs) in different fields like: - disaster management, battle ground surveillance, and border security surveillance. In such applications, a huge number of sensor nodes are deployed, which are frequently unattended and work separately. Clustering is a key technique used to expand the lifetime of a sensor network by reducing energy consumption. It can also raise network scalability. Researchers in all fields of wireless sensor network think that nodes are homogeneous, but some nodes may be of dissimilar energy to extend the lifetime of a WSN and its dependability. In this paper, we presented heterogeneous model for Wireless Sensor Network to detect intrusion and clustering algorithms proposed in the literature for heterogeneous wireless sensor networks (HWSNs).**

Keywords-; Intrusion Detection.,Reliability.,Security

I. INTRODUCTION

Wireless Sensor networks have become the one of the most attractive areas of research in the past few years. A Wireless Sensor Network is collected of a number of wireless sensor nodes that form a sensor field and a sink. These huge numbers of nodes, having the capability to sense their surroundings, perform limited calculation and communicate wirelessly appearance the WSNs. Specific functions such as sensing, tracking, and alerting as described. It can be obtained through collaboration among these nodes. These functions build wireless sensors very useful for monitoring usual phenomena, environmental changes, controlling security, estimating traffic flows, monitoring military application, and tracking friendly forces in the battlefields. These tasks need high reliability of the sensor networks. To create sensor networks extra reliable, the concentration to research on heterogeneous wireless sensor networks has been rising in recent past [1]. A sensor network can be ended scalable by assembling the sensor nodes into groups i.e. cluster. Every cluster has a leader, often referred to as the cluster head (CH). A Cluster Head may be elected by the sensors in a cluster or preassigned by the network trendy. The cluster relationship may be fixed or variable. A number of clustering algorithms have been specially designed for Wireless Sensor Networks (WSNs) for scalability and well-organized statement. The idea of cluster based routing is also exploited to present energy efficient routing in Ware less sensor networks (WSNs). In a hierarchical architecture, higher energy nodes (cluster heads) may be used to procedure and send the information even as low energy nodes may be used to achieve the sensing. Some of routing protocols in this group are: LEACH, PEGASIS, TEEN and APTEEN.

Clustering has many advantages: Some of these, which are presenting below:-

1. Clustering reduces the size of the routing table stored at the entity nodes by localizing the route set up within the cluster.
2. Clustering can preserve communication bandwidth since it restrictions the scope of inter cluster interactions to CHs and avoids superfluous exchange of messages among sensor nodes.
3. The Cluster Head (CH) can extend the battery life of the individual sensors and the network lifetime as well by implementing optimized management strategies.
4. Clustering cuts on topology preservation overhead. Sensors would care only for connecting with their Cluster Heads (CHs).
5. A CH can present data aggregation in its cluster and decrease the number of redundant packets.
6. A CH can reduce the rate of energy consumption by scheduling activities in the cluster.

Researchers generally suppose that the nodes in wireless sensor networks are homogeneous, but in reality, homogeneous sensor networks scarcely exist. Even homogeneous sensors have different Capabilities like different levels of preliminary energy, reduction rate, etc. In heterogeneous sensor networks, typically, a large number of reasonably priced nodes perform sensing, even as a few nodes having comparatively more energy perform data filtering, fusion and transport. This escort to the research on heterogeneous networks where two or more types of nodes are considered. Heterogeneity in wireless sensor networks can be used to extend the life time and reliability of the network. Heterogeneous sensor networks are popular, predominantly in real deployments as described by Freitas [2] and Corchado [3]. Most of the recent energy efficient protocols designed for heterogeneous networks are stands on the clustering technique, that are effectual in scalability and energy saving for WSNs.

II. HETEROGENEOUS MODEL OF WIRELESS SENSOR NETWORKS (WSN_S)

In this section presents a paradigm of heterogeneous wireless sensor network and converse the impact of heterogeneous resources.

2.1. Type of Resource Heterogeneity:-

There are three general types of resource heterogeneity in sensor nodes:-

- Computational Heterogeneity,
- Link Heterogeneity, and
- Energy Heterogeneity.

❖ *Computational Heterogeneity:* - Computational Heterogeneity, means that the heterogeneous node has a more powerful microprocessor, and more memory, than the normal node. With the powerful computational resources, the heterogeneous nodes can afford complex data processing and longer-term storage.

❖ *Link Heterogeneity:* - Link Heterogeneity means which the heterogeneous node has high bandwidth and long distance network transceiver than the normal node. Link heterogeneity can provide a more consistent data transmission.

❖ *Energy Heterogeneity:* - Energy Heterogeneity, means that the heterogeneous node is line powered, or its battery is expendable. Among above three types of resource heterogeneity, the mainly important heterogeneity is the energy heterogeneity since both computational heterogeneity and link heterogeneity will consume extra energy resource.

2.2. Impact of Heterogeneity on Wireless Sensor Networks:-

If we put some heterogeneous nodes in sensor network it demonstrates the following benefits:

❖ *Response Time:* - Computational heterogeneity can reduce the processing latency and link heterogeneity can reduce the waiting time, hence retort time is decreased.

❖ Lifetime: The average energy consumption will be less in heterogeneous sensor networks for forwarding a packet from the normal nodes to the sink, therefore life time is increased. Further, it is also known that if in a network, heterogeneity is used correctly then the reply of the network is tripled and the network's duration can be increased by 5fold.

2.3. Performance Measures: - Some performance measures which are used to estimate the performance of clustering protocols are scheduled below:

❖ *Network Lifetime:* - It is the time intermission from the start of operation (of the sensor network) until the death of the first alive node.

❖ *Number of Cluster Heads per Round:* - Instantaneous measure reproduces the number of nodes which would send straightly to the sink, information aggregated from their cluster members.

❖ *Number of Nodes per Round:* - This instantaneous measure reproduces the total number of nodes and that of each type that has not yet exhausted all of their energy.

❖ *Throughput:* - This comprises the total rate of data sent over the network, the rate of data sent from cluster heads to the sink as well as the rate of data sent from the nodes to their cluster heads.

III. ENERGY AWARE CONTROL STRATEGIES IN HETEROGENEOUS NETWORK

A sensor network is collected of a huge number of sensor nodes and a sink. The base-station typically provides as a entryway to some other networks. It presents powerful data processing, storage centre, and an access point to the sensor nodes in its network.

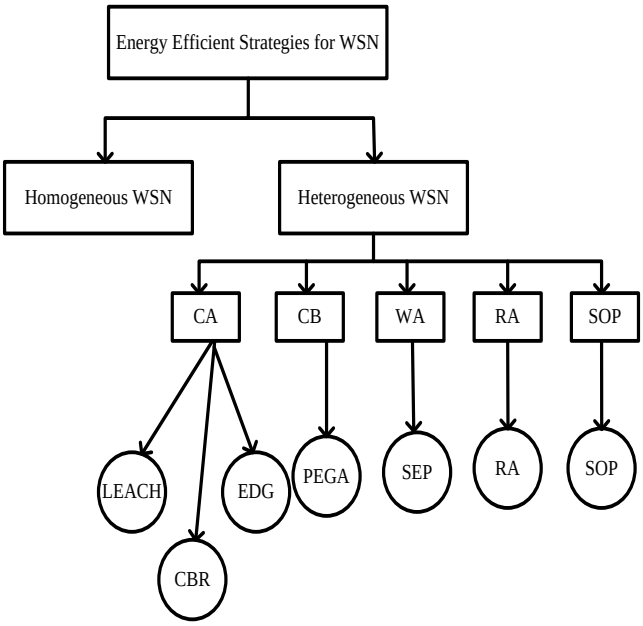

Figure.1: Taxonomy of Energy Efficient Strategies of heterogeneous WSN

CB=Chain-Based
CA=Clustering-Approach
WA=Weight-Assignment
RA=Randomized-Approach

Sensor nodes sense their environment, collect sensed data and transmit it to the BS. However, they are limited in power, computational capacity and memory. Placing few heterogeneous nodes in wireless sensor network is an effective way to increase network lifetime and reliability. Various energy efficient heterogeneous schemes have been discussed in figure 1.

IV. PRIOR STUDY WORK

Yarvis et al. [4] focused on energy and link heterogeneity in ad hoc sensor networks and consider resource-aware MAC and routing protocols to utilize those resources. Using analysis, simulation, and real test bed measurements, they evaluate the impact of number and placement of heterogeneous resources on performance in networks of different sizes and densities. While they prove that optimal deployment is very hard in general, they also show that only a modest number of reliable, long-range backhaul links and line powered nodes are required to have a significant impact. Properly deployed, heterogeneity can triple the average delivery rate and provide a 5-fold increase in the lifetime (respectively) of a large battery-powered network of simple sensors.

Krontiris et al. [5] introduced a model for distributed intrusion detection in sensor networks which is designed to work with only partial and localized information available at each node of the network. Nodes collaborate and exchange this information with their neighbors in order to make a correct decision on whether an attack has been launched. They focused their research on routing because it is the foundation of sensor networks. In particular, they demonstrated how their IDS system can be used to detect black hole and selective forwarding attacks, producing very low false-negative and false-positive rates. They also provided a set of general principles that an IDS system for sensor networks should follow.

Silva et al. [6] proposed IDS is "based on the specification", since theWSN may vary depending n the application goal. They have outlined a method for generating specific IDSs based on the target WSN that can become automatic in the future. Their detection is decentralized since the IDSs are distributed on network, installed in common nodes. The collected information and its treatment are performed in a distributed way. Distributed Systems are more scalable and robust since they have different views of the network. Besides, the IDS can notice the attack fast because the monitor is near to the intruder (their distance is one hop, since the monitors were distributed in order to cover all network nodes).

Lamport et al. [7] presented several solutions to the Byzantine Generals Problem, under various hypotheses, and shown how they can be used in implementing reliable computer systems. These solutions are expensive in both the amount of time and the number of messages required. Algorithms OM (m) and SM (m) both require message paths of length up to m 4- 1. In other words, each lieutenant may have to wait for messages that originated at the commander and were then relayed via m other lieutenants. Fischer and Lynch have shown that this must be true for any solution that can cope with m traitors, so their solutions are optimal in that respect.

Deng et al. [8] developed INSENS, a secure and Intrusion-tolerant routing protocol for wireless Sensor Networks. Redundant multipath routing improves intrusion tolerance by bypassing malicious nodes. INSENS operates correctly in the presence of (undetected) intruders. To address resource constraints, computation on the sensor nodes is offloaded to resource-rich base stations, e.g. computing routing tables, while low-complexity security methods are applied, e.g. symmetric key cryptography and one-way hash functions. The scope of damage inflicted by (undetected) intruders is further limited by restricting flooding to the base station and by having the base station order its packets using one-way sequence numbers.

Kang et al. [9] explored the problem of resilient geographic routing. Even if location information is verified, nodes may still misbehave, for example, by sending an excessive number of packets or dropping packets. To dynamically avoid untrusted paths and continue to route packets even in the presence of attacks, the proposed solution uses rate control, packet scheduling, and probabilistic multi-path routing combined with the trust-based route selection. They discussed the proposed approach in detail, outlining alternative choices. They considered possible attacks and defenses against them. In addition, they compared the performance of their resilient geographic routing protocol to a well-known geographic routing protocol.

Lou et al. [10] proposed a hybrid multipath scheme (H-SPREAD) to improve both security and reliability of this task in a potentially hostile and unreliable wireless sensor network. The new scheme is based on a distributed N-to-1 multipath discovery protocol which is able to find multiple node-disjoint paths from every sensor node to the base station simultaneously in one route discovery process. Then, a hybrid multipath data collection scheme is proposed. On the one hand, end-to-end multipath data dispersion, combined with secret sharing, enhances the security of end-to-end data delivery in the sense that the compromise of a small number of paths will not result in the compromise of a data message in the face of adversarial nodes. On the other hand, in the face of unreliable wireless links and/or sensor nodes, alternate path routing available at each sensor node improves reliability of each packet transmission significantly.

Shu et al. [11] studied routing mechanisms that circumvent (bypass) black holes formed by these attacks. They argue that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. In this paper, they also developed mechanisms that generate randomized multipath routes. Under their design, the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by their mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost. Extensive simulations are conducted to verify the validity of their mechanisms.

Karlof et al. [12] proposed security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks—sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. They describe crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.

Chan et al. [13] demonstrated that the PIKE schemes involve lower memory storage requirements than random key distribution while requiring comparable communication overheads. PIKE is currently the only symmetric-key predistribution scheme which scales sub-linearly in both communications overhead per node and memory overhead per node while being resilient to an adversary capable of undetected node compromise. PIKE enjoys a uniform communication pattern for key establishment, which is hard to disturb for an attacker. The distributed nature of PIKE also does not provide a single point of failure to attack, providing resilience against targeted attacks.

V. QOS ISSUES IN HETEROGENEOUS NETWORKS

- Administration Domain:-
  - Policy
  - Network Topology and Traffic
  - Available Services
- Access Technology
  - Mobility Suppory
  - Coverage Area
    QoS Support
  - Bandwidth, Loss and Delay
    Security
    Cost
- Terminal
  - Network Interface
  - Software Platform
- Application
  - Network Connection
  - QoS Requirement

VI. CONCLUSION

A heterogeneous network – based on a single-vendor, 3GPP-standardized and synchronized radio network with included Wi-Fi, higher traffic management and high-performance backhaul – can help distribute a consistent, high-quality and faultless mobile broadband experience. Making the right technology alternative in the right places at the right time is key to ensuring smooth capacity expansion with maximum efficiency. Operators are able to influence their existing, established 3GPP network and terminal base, by civilizing, densifying and adding to the macro communications to meet surging traffic demand. In this paper, we have presented the overview of wireless sensor network and Heterogeneous. We also demonstrated the heterogeneous model of wireless sensor network

VII. REFERENCES

[1]ChunHsien W., and YehChing C., "Heterogeneous Wireless Sensor Network Deployment and Topology Control Based on Irregular Sensor Model", Advances in Grid and Pervasive Computing Lecture Notes in Computer Science. 4459, 2007

[2]DeFreitas, E.P., Heimfarth, T. and Pereira, C.E, "Evaluation of coordination strategies for heterogeneous sensor networks aiming at surveillance applications", In: Proceedings of IEEE Sensors (SENSORS), Christchurch, Newzealand, pp.591–596, 2009

[3]Corchado, J.M., Bajo, J., Tapia, D.I. and Abraham, A, "Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare", IEEE Transactions on Information Technology in Biomedicine, Vol.14 (2), pp 234–240, 2010

[4] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in Proc. 2005 IEEE Conf. Computer Commun., vol. 2, pp. 878–890.

[5] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 2007 European Wireless Conf

[6] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proc. 2005 ACM Workshop Quality Service Security Wireless Mobile Netw.

[7] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem, "ACM Trans. Programming Languages Syst., vol. 4, no. 3, pp. 382–401, 1982

[8] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," Computer Commun., vol. 29, no. 2, pp. 216–230, 2006.

[9] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in Proc. 2006 Cyber Security Conf. Inf. Assurance.

[10] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320–1330, 2006

[11] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, 2010.

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proc. 2003 IEEE Int. Workshop Sensor Netw. Protocols Appl., pp. 113–127.

[13] C. Haowen and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks," in Proc. 2005 IEEE Conf. Computer Commun., pp. 524–535.