ISSN:0975-9646

Trustworthy and Energy-Saving Measures in Wireless Sensor Networks by using Multipath Routing

Arun Kumar. S

Research Scholar, CMR University, India

***Abstract*— In a heterogeneous networks responsibility of tolerant topology control consisting of numerous reserve affluent super nodes in the wireless networks used for information dispatching and a huge number of vigour constrained wireless sensor nodes. In this paper we executed a performance trade-off analysis of energy consumption vs. Quality of Services gain in reliability, appropriateness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. We urbanized a novel probability model to analyze the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best intrusion recognition settings in terms of the number of voters (m) and the intrusion incantation interval under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. Finally, we applied our analysis results to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime. For future work, we plan to explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behaviour and collude with other attackers to avoid intrusion detection. Lastly, we plan to investigate the use of trust/reputation management to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes, as well as to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs. In situations where concurrent query traffic is heavy, we plan to explore trust-based admission control to optimize application performance.**

***Keywords*— Heterogeneous wireless sensor networks; multipath routing; intrusion detection; reliability; security; energy conservation**

I. INTRODUCTION

Heterogeneous Wireless Networks is composed of a large number of low-cost devices distributed over a geographic area. Sensor nodes have limited processing capabilities; therefore simplified protocol architecture should be designed so as to make communications simple and efficient. Moreover, usually the power supply unit is based on an energy-limited battery; therefore solutions elaborated for these networks should be aimed at minimizing the energy consumption. To this purpose, several works have shown that energy consumption is mainly due to data transmission, and accordingly energy conservation schemes have been proposed aimed at minimizing the energy consumption of the radio interface. With the aim of reducing energy consumption while taking the algorithmic complexity into account, we propose a novel approach that splits the original messages into several packets such that each node in the network will forward only small sub packets. The splitting procedure is achieved applying the Chinese Remainder Theorem (CRT) algorithm, which is characterized by a simple modular division between integers. The sink node, once all sub packets (called CRT components) are received correctly, will recombine them, thus reconstructing the original message. The splitting procedure is especially helpful for those forwarding nodes that are more solicited than others due to their position inside the network. Regarding the complexity, in the proposed approach, almost all nodes operate as in a classical forwarding algorithm and, with the exception of the sink, a few low-complex arithmetic operations are needed. If we consider that the sink node is computationally and energetically more equipped than the other sensor nodes, the overall complexity remains low and suitable for a WSN.

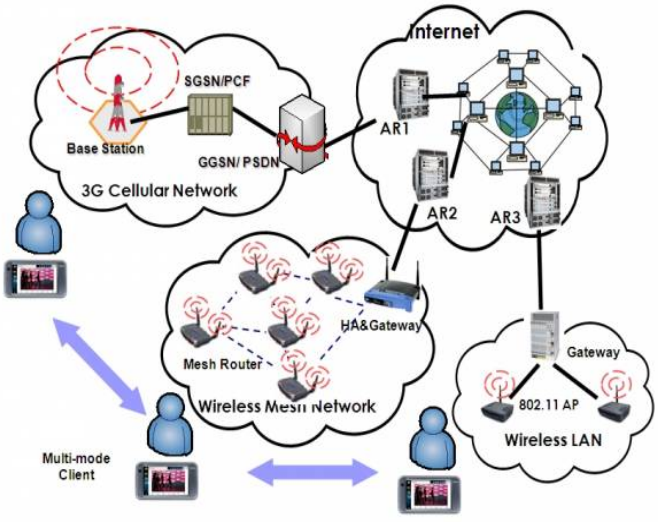

Fig-1 Architecture of Heterogeneous WSN

A Wireless ad hoc sensor networks (WSNs) assuring many new exciting applications in the future, such an everywhere on-demand computing supremacy, incessant

connectivity, and instantaneously deployable communication for armed and responders. These types of wireless sensor networks already help to observe critical environmental conditions in volcanic eruption areas, underwater and so on; factories maintenance works, and troop utilization, to name a few applications. As WSNs grow to be a greater extent essential to the everyday performance of people and organizations and also many attacks are arising in the wireless ad hoc networks.

For effective redundancy managements authors proposed many schemes to address the energy consumption in the networks. In Existing System, effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious node is needed. More specifically, we analyse the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. But some obstacles interrupt the networks efficiency in different ways such as the increasing packet delay, thus time consuming for reordering the packets, Optimization is not effectively handled also Buffering problem in low bandwidth data thus reduces efficiency. In order to overcome the disadvantages of the previously proposed system, we implement the new idea in this paper.

In our proposed system, the best possible contact range and communication method were derivative to utilize the Heterogeneous Wireless Sensor Networks existence in nature. In HWSN, the intra-cluster scheduling and inter-cluster multi-hop routing proposal to capitalize the network lifetime. And it is considered as a hierarchal HWSN with CH nodes including superior energy and giving out capabilities than normal SNs. Our proposed technique gives solution to formulate as an optimization difficulty to balance energy consumption across all nodes in the entire heterogeneous sensor networks. Though in this paper, we suggest two-tier HWSN with the intention of capitalizing on network lifetime while fulfilling power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime.

The rest of the paper will be organised as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The algorithms and simulation are shown in the section 4 and 5. The conclusion of our paper is in section 6.

II. RELATED WORKS

In this section, we will see the some of the related works to the wireless ad hoc networks using different approaches:

Matthias Grossglauser and David N. C. Tse [1], the capability of ad hoc wireless networks is forced by the common intrusion of concomitant communication between the two nodes. We study a model of a wireless ad hoc network where nodes correspond in arbitrary to the resource–target pairs. These wireless nodes are tacit to be mobile for the communication networks. We examine the each and every session throughput for the wireless network applications with variable stoppage constraints, such a wireless network topology changes or clear in excess of the instant scale of packet or data's delivery. Under this statement, the per-user throughput can augment radically when nodes are movable moderately than fixed. This development can be achieved through by exploiting an appearance of multiuser multiplicity via sachet or information relaying between the two different nodes.

An energy-efficient distributed [2] clustering approach for ad-hoc sensor networks. This approach is hybrid: cluster heads are randomly selected based on their residual energy, and nodes join clusters such that communication cost is minimized. Based on this approach, authors have introduced the HEED protocol, which terminates in a constant number of iterations, independent of the network diameter. HEED operates in quasi-stationary networks where nodes are location-unaware and have equal significance. No assumptions are made about the node dispersion or density in the field. Simulation results show that HEED prolongs network lifetime, and the clusters it produces exhibit several appealing characteristics. HEED parameters, such as the minimum selection probability and network operation interval, can be easily tuned to optimize resource usage according to the network density and application requirements. HEED can also be useful in multi-hop networks if the necessary conditions for connectivity (the relation between cluster range and transmission range under a specified density model) hold. This approach can be applied to the design of several types of sensor network protocols that require energy efficiency, scalability, prolonged network lifetime, and load balancing. Although it has provided a protocol for building a single cluster layer, it can extend the protocol to multi-level hierarchies. This can be achieved by recursive application at upper tiers using bottom-up cluster formation. We are currently investigating cluster size constraints in HEED.

Novel packet delivery mechanism [3] called Multi-Path and Multi-SPEED Routing Protocol (MMSPEED) for probabilistic QoS guarantee in wireless sensor networks. The QoS provisioning is performed in two quality domains, namely, timeliness and reliability. Multiple QoS levels are provided in the timeliness domain by guaranteeing multiple packet delivery speed options. In the reliability domain, various reliability requirements are supported by probabilistic multipath forwarding. These mechanisms for QoS provisioning are realized in a localized way without global network information by employing localized geographic packet forwarding augmented with dynamic compensation, which compensates for local decision inaccuracies as a packet travels towards its destination. This way, MMSPEED can guarantee end-to-end requirements in a localized way, which is desirable for scalability and adaptability to large scale dynamic sensor networks.

Zinaida benenson , Peter M. cholewinski and, Felix C. freiling [4], We examine how wireless ad hoc networks can be attacked in follow. Beginning of this, we extend our

previous idea of generic rival model that allows classifying the adversaries according to the two extent of power: presence and intervention. Thus, we provide a framework for realistic safety measures analysis in wireless sensor or ad hoc networks

Chris Karlof and David Wagner [5], we examine the routing protocol security in wireless networks. Many wireless sensor network routing protocols comprise be proposed in previous, but nothing of them have been considered with security as a goal in the wireless networks. We propose the effective protection goals for routing protocols in the sensor networks, show how attacks beside ad-hoc and end to end networks can be adapted into dominant attacks against sensor networks, initiate two classes of novel attacks touching sensor networks — sinkholes and HELLO floods, and we analyse that the security of all the major sensor network routing protocols. We illustrate crippling attacks against all of them and propose countermeasures and aim for considerations. This is the first such examine of secure routing in wireless sensor networks.

Farhad Nematy , and Naeim Rahmani [6], in modern years there has been a growing consideration in wireless ad hoc sensor networks (WSN) applications. Such wireless sensor networks are able to be second-hand to manage temperature in the desert or volcanic regions, humidity, contamination, pollution etc. Energy utilization and dependability are two serious issues in WSNs. Faults or Misbehaviour occurring to sensor nodes is frequent owing to be short of power or ecological intrusion. In this paper recovery of faults nodes or misbehaviour in cluster beginning deliberate and genetic system is used to recuperate huddle members to other cluster heads. Our Simulation results show effectiveness that proposed genetic algorithm can recover the fault nodes efficiently.

Dr. G. Padmavathi, and Mrs. D. Shanmugapriya,[7], Wireless Sensor networks (WSN) is an rising technology and have immense credible to be betrothed in significant situation like battlefields surveillance, marketable applications such as construction, travel examination, environment monitoring and well-groomed homes and several additional scenarios. Smart environments correspond to the subsequently evolutionary expansion rung in building or homes, utilities, manufacturing purposes, residence, shipboard, and shipping systems mechanization. Similar to several conscious creatures, the elegant surroundings relies initial and leading on sensory data or information as of the genuine humanity. Such a Sensory data or information comes as of numerous sensors of unlike modalities in scattered surroundings. The elegant atmosphere desires in order about its environment because well about its interior mechanism; so it is captured in natural systems by the dissimilarity among the one is ext-eroceptors and other is pro-prioceptors. In the wireless communication technologies also acquire various types of security intimidation. This paper deals with an extensive diversity of attacks or privacy issue in WSN and their categorization techniques and applying dissimilar securities levels available to feel them as well as the challenges or issues faced in WSN.

Chaudhari H.C. and Kadam L.U [8], however, wireless sensor networks pretense exclusive protection challenges. Security is fetching a major anxiety for WSN protocol designers as of the extensive security serious applications of WSNs protocols. we include completed an attempt to document all the recognized security issues in wireless sensor networks and discuss a deals with an extensive diversity of attacks or privacy issue in WSN and their categorization techniques and applying dissimilar securities levels available to feel them as well as the challenges or issues faced in WSN. In this paper we took up the challenge or issues in the security level and have proposed an included wide-ranging security that will present security services for all services of sensor network. The sensing technology shared with processing control and wireless communication makes it gainful for being broken in great measure in future. The wireless communication technologies also acquire various types of security intimidation.

Proposed Work

For effective redundancy managements the authors proposed many schemes to address the energy consumption in the networks. In Existing System, effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes; More specifically, we analyse the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. But some obstacles interrupted the networks efficiency in different ways such as the increasing packet delay, thus time consuming for reordering the packets, Optimization is not effectively handled and Buffering problem in low bandwidth data, thus reducing efficiency. In order to overcome the disadvantages of the previously proposed system, we implement the new idea in this paper.

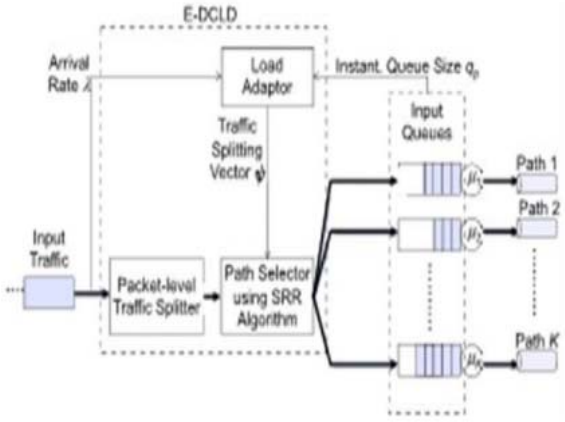

Figure 2- Proposed Architecture

In this our proposed system, the best possible contact range and communication method were derivative to utilize

the Heterogeneous Wireless Sensor Networks existence in nature. In HWSN, the intra-cluster scheduling and inter-cluster multi-hop routing proposal to capitalize the network lifetime. And it is considered as a hierarchal HWSN with CH nodes including superior energy and giving out capabilities than normal SNs. Our proposed technique gives solution to formulate as an optimization difficulty to balance energy consumption across all nodes in the entire heterogeneous sensor networks. Though in this paper, we suggest two-tier HWSN with the intention of capitalize on network lifetime while fulfilling power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime.

III. ALGORITHM

CH Execution:
Get next event
if event is T_D timer **then**
    determine radio range to maintain CH connectivity
    determine optimal T_{IDS}, m, m_s, m_p by
      table lookup based on the current estimated
      density, CH radio range and compromise rate
    notify SNs within the cluster of the new
      optimal settings of T_{IDS} and m
else if event is query arrival **then**
    trigger multipath routing using m_s and m_p
else if event is $T_{clustering}$ timer **then**
    perform clustering
else if event is T_{IDS} timer **then**
    For each neighbor CH
      if selected as a voter **then**
        execute voting based intrusion detection
else // event is data packet arrival
    follow multipath routing protocol design to route

SN Execution:
Get next event
if event is T_D timer **then**
    determine radio range to maintain SN connectivity
      within a cluster
else if event is control packet arrival from CH **then**
    Change the optimal settings of T_{IDS}, and m
else if event is $T_{clustering}$ timer **then**
    perform clustering
else if event is T_{IDS} timer **then**
    For each neighbor SN
      if selected as a voter **then**
        execute votingbased intrusion detection
else // event is data packet arrival
    follow multipath routing protocol design to route
      the data packet

IV. SIMULATION WORKS/RESULTS

Multi – Path Routing:

In this module, Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of atleast one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoffs' between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

User Interface:

In this module, we have to create the user interface for establishing the connection between the sender and the receiver. Here the user has to prepare the data that has to send to the particular destination. For every transaction, user interface is the main part for establishing connection between the sender and the receiver. After establishing the connection, the sender has to prepare for the data, which he wants to send to the particular destination.

Calculate the path feature:

In this module, the path feature has to calculated by load adapter to minimize the path delay and packet delay, thus minimizing the time consuming for reordering the packets at the destination. This information has to send to the traffic splitting component and path selector component. The path calculating is based on the load balancing server called cell breathing server, which effectively find the path feature by using multipath communication.

Splitting the packets:

According to the path information that is sent by the load adapter, the packet will be spitted to send across the path

Path Selection:

The spitted packets are sent to the path selector component, according to the path information, the path selector component will choose the path and send the packet through the network.

Reordering the packets:

After receiving the packets, the packets are reordering in the destination in an efficient manner, thus minimizing the delay for reordering the packets.

Intrusion Tolerance:

In this Module, intrusion tolerance through multipath routing, there are two major problems to solve:

(1) How many paths to use and

(2) What paths to use.

To the best of our knowledge, we are the first to address the "how many paths to use" problem. For the "what paths to use" problem, our approach is distinct from existing work in that we do not consider specific routing protocols.

Energy Efficient:

In this module, there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach especially applicable to flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach which we adopt in this paper is to use local host -based IDS for energy conservation.

V. CONCLUSION

Our proposed techniques in this paper, address the properties of routing path energy consumption and tolerance obstacles in the wireless ad hoc networks. A Tradeoffs analysis of energy consumption vs QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. We developed a novel probability model to analyse the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best intrusion detection settings in terms of the number of voters (m) and the intrusion invocation interval (TIDs) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. Our experimental result showed that our proposed novel technique works efficiently when compared to previous methods.

REFERENCES

[1] Matthias Grossglauser and David N. C. Tse "Mobility Increases the Capacity of Ad Hoc Wireless Networks"- IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 10, NO. 4, AUGUST 2002

[2] Shuo Guo, Ziguo Zhong and Tian He "FIND: Faulty Node Detection for Wireless Sensor Networks"- SenSys'09, November 4–6, 2009, Berkeley, CA, USA

[3] B. Umakanth and J. Damodhar "Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks"- International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013.

[4] Zinaida benenson , Peter M. cholewinski and, Felix C. freiling "Vulnerabilities and Attacks in Wireless Sensor Networks"

[5] Chris Karlof and David Wagner proposed "Trust Evaluation Based Security Solution in Ad Hoc Networks"

[6] Farhad Nematy , and Naeim Rahmani "A New Approach for Recovering Nodes from Faulty Cluster Heads Using Genetic Algorithm"- Proceedings of the International Conference on Soft Computing for Problem Solving (SocProS 2011) December 20-22, 2011

[7] Dr. G. Padmavathi, and Mrs. D. Shanmugapriya "Simulation of a Secure Ad Hoc Network Routing Protocol"- (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009

[8] Chaudhari H.C. and Kadam L.U "Security in Ad Hoc Networks"- International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16.

[9] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks,"Proc. ACM MobiCom,2004.

[10] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks,"IEEE Trans. Mobile Computing,vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[11] T. Aura, "Dos-Resistant Authentication with Client Puzzles,"Proc. Int'l Workshop Security Protocols,2001.

[12] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,"Proc. 12th Conf. USENIX Security,2003.

[13] D. Bernstein and P. Schwabe, "New AES Software Speed Records,"Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT),2008.

[14] D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html,1996.

[15] I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography,vol. 265. Cambridge Univ., 1999.

[16] J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[17] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks,"Computer,vol. 36, no. 10, pp. 103-105, Oct. 2003.

[18] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks,"IEEE/ACM Trans. Networking,vol. 12, no. 4, pp. 609-619, Aug. 2004.

[19] T.H. Clausen and P. Jacquet,Optimized Link State Routing Protocol (OLSR),IETF RFC 3626, 2003.

[20] J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks,"Proc. ACM Workshop Security of Ad Hoc and Sensor Networks,2005.

[21] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks,"Computer Comm.,vol. 29, no. 2, pp. 216-230, 2006.

[22] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network,"ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.