IJMEIT
IGM Publication
International Journal Of Mechanical Engineering And Information Technology
An Official Publication Of IGM Publication

Weighted Voting based Trust Management for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks

P.Swaruba[1], K.Kumaresan[2]

Email id:swarubait@gmail.com

Abstract:

Heterogeneous wireless sensing element network (heterogeneous WSN) consists of sensing element nodes with totally different ability, like totally different computing power and sensing vary. Compared with homogenised WSN, readying and topology management square measure additional advanced in heterogeneous WSN. The present work bestowed redundancy management of heterogeneous wireless sensing element network s (HWSNs), utilizing multipath routing to answer user queries in presence of unreliable and malicious nodes. Redundancy management exploits trade-off between energy consumption against gain in responsibleness and timeliness and security to maximise system helpful period of time. It's optimality is arrived to dynamically confirm the most effective redundancy level to use to multipath routing for intrusion tolerance. The question response success chance is maximized and also the life time is prolonged. Voting-based distributed intrusion discoverion formula was applied to detect and evict malicious nodes in HWSN. The chance model was analyzed with the most effective redundancy level in terms of path redundancy and supply redundancy.The projected work bestowed weighted vote primarily based Trust Management theme to boost the performance of intrusion tolerance in HWSN. The Trust model permits every sensing element node to guage trustiness of neighbor in HWSN region of section. Weighted vote is introduced to all or any the neighbor nodes supported name count worth of corresponding sensing element node. Simulations were conducted on totally different sensing element nodes to live the performance in terms of. The projected work

showed an improvement of in comparison to the present.

***Keywords**: Intrusion Detection Network, Wireless sensing element Network, Multipath Routing, Trust Management*

I. INTRODUCTION

A wireless sensing element network (WSN) consists of spatially distributed autonomous sensors to watch physical or environmental conditions, like temperature, sound, pressure, etc. and to hand and glove pass their knowledge through the network to a main location. The additional fashionable networks square measure bi-directional, additionally facultative management of sensing element activity. The accuracy of police investigation AN intrusion at intervals a network of intrusion detection systems (IDSes) depends on the potency of collaboration between member IDSes. the safety itself at intervals this network is a further concern that must be addressed . several wireless sensing element networks (WSNs) square measure deployed in AN unattended surroundings during which energy replacement is troublesome if not not possible. owing to restricted resources, a WSN should not solely satisfy the applying specific QoS necessities like responsibleness, timeliness and security, however additionally minimize energy consumption to prolong the system helpful period of time. The trade-off between energy consumption vs. responsibleness gain with the goal to maximise the WSN system life time has been well explored within the literature. However, no previous work exists to contemplate the trade-off within the presence of malicious attackers.

A trust-based framework for secure ANd effective collaboration at intervals an intrusion detection network (IDN). particularly, we tend to outline a trust model that permits every IDS to guage the trustiness of others supported personal expertise. we tend to prove the correctness of our approach in protective the IDN. in addition, experimental results demonstrate that our system yields a big improvement in police investigation intrusions. The trust model more improves the lustiness of the cooperative system against malicious attacks.

Intrusions over the web have become additional dynamic and complicated. Intrusion Detection Systems (IDSes) determine intrusions by scrutiny noticeable behavior against suspicious patterns. they'll be network-based (NIDS) or host-based (HIDS). ancient IDSes add isolation and will be simply compromised by unknown or new threats. AN Intrusion Detection Network (IDN) may be a cooperative IDS network supposed to beat this weakness by having every members IDS have the benefit of the collective data and knowledge shared by different member IDSes. This enhances their overall accuracy of intrusion assessment in addition because the ability of police investigation new intrusion varieties.

Multipath routing is taken into account a good mechanism for fault and intrusion tolerance to boost knowledge delivery in WSNs. the fundamental plan is that the chance of a minimum of one path reaching the sink node or base station will increase as we've additional methods doing knowledge delivery. A HWSN includes sensors of various capabilities. we tend to contemplate 2 sorts of sensors: CHs and SNs. CHs square measure superior to SNs in energy and machine resources.

The trust management schemes incorporates a robust tool for the detection of surprising node behaviors (either faulty or malicious). Once misbehaving nodes square measure detected, their neighbors will use this info to avoid cooperating with them, either for knowledge forwarding, knowledge aggregation or the other cooperative operate. a strong trust management model that's appropriate for distributed HIDS collaboration. Our model permits every HIDS to guage the trustiness of others supported its own expertise with them. we tend to additionally propose a framework for economical HIDS collaboration employing a peer-to-peer network. Our framework provides identification for taking part HIDSes and creates incentives for collaboration amongst them.

The trust models in an effort to explore the interaction among the implementation necessities, the resource consumption and also the achieved security. Our goal is to draw guidelines for the planning of deployable trust model styles with relation to the obtainable node and network capabilities and application peculiarities.

II. LITERATURE REVIEW

Over the past few years, many protocols exploring the exchange between energy consumption and QoS gain notably in reliableness in HWSNs ar projected. In [19], the most effective communication varies and communication modes were derived to maximise the HWSN amount.

In [1] the accuracy of police investigation intrusions at intervals AN Intrusion Detection Network (IDN) depends on the potency of collaboration between the peer Intrusion Detection Systems (IDSes) in addition because the security itself of the IDN against corporate executive threats. Intrusion Detection Systems (IDSes) determine intrusions by scrutiny noticeable behavior against suspicious patterns. they'll be network-based (NIDS) or host-based (HIDS). ancient IDSes add isolation and will be simply compromised by unknown or new threats. AN Intrusion Detection Network (IDN) may be a cooperative IDS network supposed to beat this weakness by having every peer IDS have the benefit of the collective data and knowledge shared by different peers. This enhances the general accuracy of intrusion assessment in addition because the ability of police investigation new intrusion kind.

In [2] a good cooperative Intrusion Detection Network (CIDN) permits distributed Intrusion Detection Systems (IDSes) to collaborate and share their data and opinions concerning intrusions, to reinforce the general accuracy of intrusion assessment in addition because the ability of police investigation new categories of intrusions a distributed Host primarily based IDS (HIDS) collaboration system, notably specializing in acquaintance management wherever every HIDS selects and maintains a listing of collaborators from that they'll consult concerning intrusions. additional specifically, every HIDS evaluates each the false positive (FP) rate and false negative (FN) rate of its neighboring HIDSes' opinions concerning intrusions victimization Bayesian learning, and aggregates their opinions concerning intrusions employing a

Bayesian call model. Our dynamic acquaintance management formula permits every HIDS to effectively choose a group of collaborators. we tend to measure our system supported a simulated cooperative HIDS network.

In [3] A distributed theme supported sharing info between trustworthy peers in a very network to protect the network as an entire against intrusion makes an attempt. we tend to gift initial concepts for running Hindu deity over a peer-to-peer infrastructure to distribute up-to-date rumors, facts, and trust info in a very ascendible manner. Intrusion is that the act or tried act of employing a ADP system or laptop resources while not the requisite privileges, inflicting willful or incidental harm. Intrusion detection involves distinguishing people or machines that perform or try intrusion. Intrusion Detection Systems (IDS) square measure laptop programs that commit to perform intrusion detection by scrutiny noticeable behavior against suspicious patterns, ideally in time period. Intrusion is primarily a network primarily based activity.

In [4] The proliferation of laptop viruses and net worms has had a significant impact on the web Community. Cleanup and management of malicious code (malware) has become a key drawback for network directors. Effective techniques square measure currently required to shield networks against outbreaks of malware. Wire-speed firewalls are wide deployed to limit the flow of traffic from untrusted domains. however these devices weakness resides in a very restricted ability to shield networks from infected machines on otherwise trustworthy networks. Progressive network directors are victimization AN Intrusion hindrance System (IPS) to actively block the flow of malicious traffic. New sorts of active and extensile network systems that use each microprocessors and reconfigurable logic will perform wire-speed services so as to shield networks against bug and net worm propagation.

In [5] Distributed networks depend upon collaboration among distributed entities. to reinforce security in distributed networks, like impromptu networks, it's necessary to guage the trustiness of taking part entities since trust is that the major drive for collaboration. during this paper, we tend to gift a framework to quantitatively live trust, model trust propagation, and defend trust analysis systems against malicious attacks.

In specific, we tend to address the basic understanding of trust, quantitative trust metrics, mathematical properties of trust, dynamic properties of trust, and trust models.

The attacks against trust analysis square measure known and defense techniques square measure developed. The projected trust analysis system is utilized in impromptu networks for securing impromptu routing and helping malicious node detection. The implementation is totally distributed. Simulations show that the projected system will considerably improve the network outturn in addition as effectively discover malicious behaviors in impromptu networks.

In [6] many varieties of network intrusions occur in multiple networks at the same time, as an example, scanning, worms, and denial-of-service attacks. Most of the present intrusion discoverion systems add isolation to detect these attacks. Past analysis has shown that collaboration between these networks to share suspicious info is a good thanks to discover intrusion. However, there square measure some challenges related to the concept of cooperative detection, like quantifiability and rejection of a central purpose of failure. we tend to propose a peer-to-peer approach for cooperative intrusion detection to deal with these challenges. Our answer proposes secure knowledge sharing between participants from totally different organizations employing a content primarily based peer-to-peer publish/subscribe mechanism. The projected theme improves quantifiability, whereas avoiding a central purpose of failure.

In [7] Intrusion Detection is sensing element networks and that we propose a light-weight theme which will be applied to such networks. Its basic characteristic is that nodes monitor their neighborhood and collaborate with their nearest neighbors to bring the network back to its traditional operational condition. we tend to emphasize in a very distributed approach during which, even if nodes don't have a worldwide read, they'll still discover AN intrusion ANd manufacture an alert. we tend to apply our style principles for the part and selective forwarding attacks by process applicable rules that characterize malicious behavior. Intrusion Detection design permits them to require management of the data flowing within the network. Besides, sensing element networks square measure in the main concerning reportage knowledge back to the bottom station, and disrupting this method would create AN attack a winning one.

In [8] Wireless sensing element networks (WSNs) have several potential applications. it's necessary to use some mechanism of intrusion detection. Besides preventing the entrant from inflicting damages to the network, the intrusion detection system (IDS) will acquire info associated with the attack techniques, serving to the event of hindrance systems. during this work we tend to propose IDS that matches the strain and restrictions of WSNs. Simulation results reveal that the projected IDS is economical and correct in police investigation totally different types of simulated attacks. The followings steps should be taken to construct AN applicable IDS to a target WSN: (1) pre-select, from the obtainable set of rules, people who are often accustomed monitor the options outlined by {the style|the planning|the look}er; (2) compare the data needed by the pre-selected rules with the data obtainable at the target network to pick out rules definitively; and (3) set the parameters of the chosen rules with the values of the design definitions.

In [9] Mobile impromptu networks and wireless sensing element networks have secure a large kind of applications. However, they're usually deployed in doubtless adverse or maybe hostile environments. Therefore, they can't be without delay deployed while not initial addressing security challenges. Intrusion detection systems give a necessary layer of in-depth protection for wired networks. However, comparatively very little analysis has been performed

about intrusion detection within the areas of mobile impromptu networks and wireless sensing element networks. Then we tend to specialise in their intrusion detection capabilities. Specifically, we tend to gift the challenge of constructing intrusion detection systems for mobile impromptu networks and wireless sensing element networks, survey the present intrusion detection techniques, and indicate necessary future analysis directions.

In [10] Communication security and responsibleness square measure 2 necessary problems in any network. A typical communication task in a very wireless sensing element network is for each sensing element node to sense its native surroundings and, upon request, sends knowledge of interest back to a base station. during this paper, we tend to propose a hybrid multipath theme (H-SPREAD) to boost each security and responsibleness of this task in a very doubtless hostile and unreliable wireless sensing element network. The new theme is predicated on a distributed N-to-1 multipath discovery protocol that is in a position to search out multiple node-disjoint methods from each sensing element node to the bottom station at the same time in one route discovery method. Then, a hybrid multipath knowledge assortment theme is projected. On the one hand, end-to-end multipath knowledge dispersion, combined with secret sharing, enhances the safety of end-to-end knowledge delivery within the sense that the compromise of atiny low variety of methods won't lead to the compromise of an information message within the face of adversarial nodes. On the opposite hand, within the face of unreliable wireless links and/or sensing element nodes, alternate path routing obtainable at every sensing element node improves responsibleness of every packet transmission considerably.

III. SYSTEM MODEL

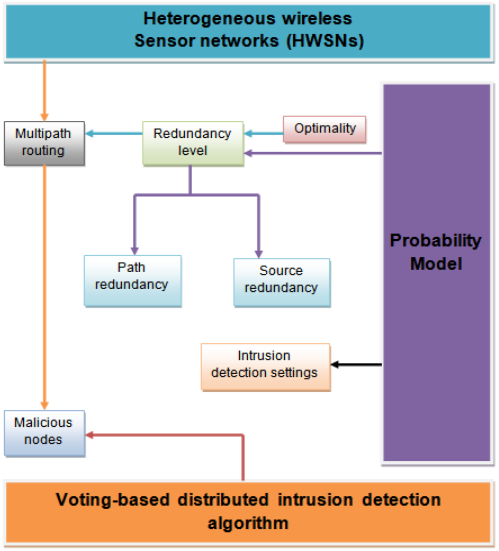

Fig 2. Overall performance architecture of system model

The phases concerned within the projected theme are:

- Neighbor Node name Estimation

- Neighbor Node with Random Poisson
- Weighted vote for Trust management
- Weighted vote Intrusion Tolerant

A. Neighbor Node Random Poisson

The Neighbor node name estimation analysis of trustiness of a node is disbursed victimization take a look at messages sent out sporadically employing a random Poisson method. when a node receives feedback for AN alert analysis it assigns satisfaction worth to that i.e., terribly glad, Satisfied, Neutral, unhappy terribly unhappy.

Trust worth of every node is updated supported the satisfactory levels of its feedback. The replies obtained from the node square measure ordered from most up-to-date to oldest in keeping with time at that it had been received by neighbor node feedback.

B. Neighbor Node name Estimation

Neighbor Node name Estimation (NNRE) alters attainable changes of node behavior over time use forgetting issue. It helps in assignment less weight to older feedback responses. It uses multiple satisfaction levels that doesn't forget recent experiences exponentially to permit a node to send a “don’t know” answer to asking if it's no expertise with alert or isn't assured with its ranking call it encourages the nodes to supply satisfactory feedback responses. or else, the trust worth slowly updated whenever node provides a don’t apprehend answer.

C. Weighted vote for Trust management

Weighted vote for trust management is predicated on the history of trustiness of every node requests alert consulting solely from those nodes in its acquaintance list whose trust values square measure larger than a threshold. It considers proximity of a live of physical distance between node that gives feedback and node that sends request. Physical location is one in all the necessary parameter in intrusion detection.

Node Intrusions placed in same or obtainable countryside square measure doubtless to expertise similar intrusions. It helps one another by broadcasting warnings of active threats.

D. Weighted vote Intrusion Tolerant

Feedback from near acquaintances is additional relevant than from distant ones. The proximity is scaled supported the region node that belongs to region level. when receiving feedback from its acquaintances node it aggregates the feedback victimization weighted majority technique.

It manages multipath routing for intrusion tolerance to maximise the system period of time. It additionally management actions taken by individual SNs and CHs in response to dynamically dynamic environments

Once an information packet arrival event happens every node merely follows prescribed multipath routing protocol to route the packet. Every node sporadically performs bunch.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

During this section we tend to measure performance of weighted vote primarily based trust management for intrusion tolerance in heterogeneous wireless sensing element networks through NS2 simulation. to verify the analytical results, we tend to enforced Weighted vote {based|based mostly|primarily primarily based} trustworthy Technique within the sensing element networking machine ns-2 and evaluated weighted vote based trust management the performance of technique.

The performance of is evaluated by the subsequent metrics.

- Size of correct Ranking
- Trust worth of Malicious Nodes
- No of Infected Nodes

Table 1.Size of Ranking

NUMBER OF NODE	SIZE OF RANKING IN EXISTING SYSTEM	SIZE OF RANKING IN PROPOSED SYSTEM
10	45	40
20	49	45
30	53	50
40	58	53
50	61	59

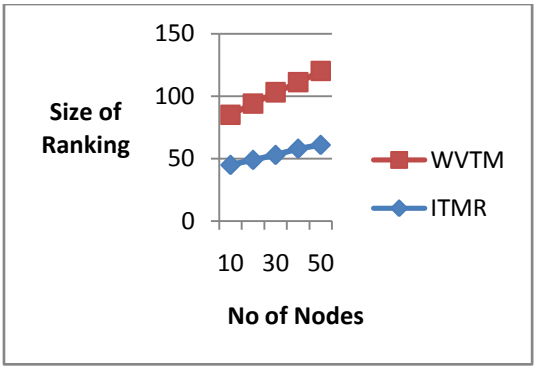

Fig 1. Size of correct Ranking

Figure 1 demonstrates the dimensions of correct Ranking. X axis represents the amount of nodes whereas Y axis denotes the dimensions of Ranking victimization each the projected weighted vote primarily based trust Management. once the amount of nodes enlarged, Size of Ranking rate gets decreases consequently. the speed of Size of Ranking is illustrated victimization the present Intrusion tolerant multipath routing and projected weighted vote primarily based trust Management. Figure two shows higher performance of projected weighted vote {based|based mostly|primarily primarily based} trust Management in terms of No of nodes density than existing and projected weighted vote based trust Management. Weighted vote primarily based trust Management achieves fifteen to twenty fifth less Size of Ranking rate variation in comparison with existing system

Table 2: Trust Value of Malicious Node

NUMBER OF NODE	TRUST VALUE OF MALICIOUS NODE IN EXISTING SYSTEM	TRUST VALUE OF MALICIOUS NODE IN PROPOSED SYSTEM
10	1	0.25
20	8	6
30	9	7
40	13	10
50	20	16

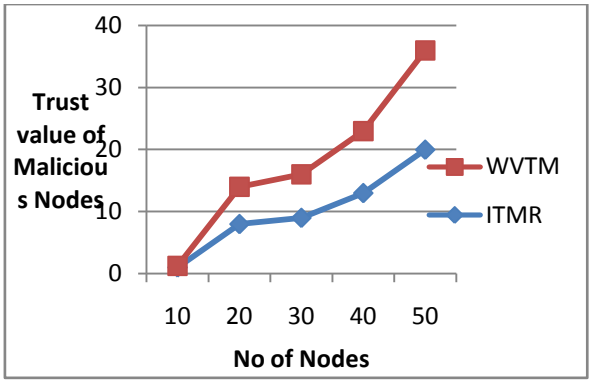

Fig 2. Trust Value of Malicious Nodes

Figure 2 demonstrates the Trust worth of Malicious Nodes. X axis represents the amount of nodes whereas Y axis denotes Trust worth of Malicious Nodes the victimization each the Intrusion detection multipath Routing and our projected Weighted vote primarily based trust Management. once the amount of nodes enlarged, Trust worth of Malicious Nodes additionally gets will increase consequently. The Trust worth of Malicious Nodes is illustrated victimization the present Intrusion detection multipath Routing and our projected Weighted vote primarily based trust Management. Figure three shows higher performance of projected Weighted vote {based|based mostly|primarily primarily based} trust Management in terms of nodes than existing Intrusion detection multipath Routing and our projected Weighted vote based trust Management. Weighted vote primarily based trust Management achieves twenty to thirty fifth less Trust worth of Malicious Nodes variation in comparison with existing system.

Table 3: No of Infected Nodes

NUMBER OF NODE	NO OF INFECTED NODES IN EXISTING SYSTEM	NO OF INFECTED NODES IN PROPOSED SYSTEM
10	6	4
20	5	3
30	4	2
40	3	1
50	2	0.025

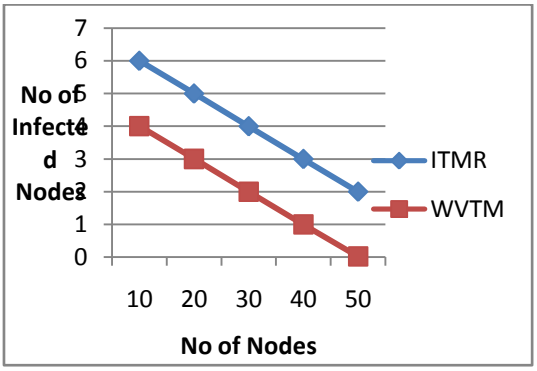

Fig 3. No of Infected Nodes

Figure 3 demonstrates the No of Infected Nodes. X axis represents variety of nodes whereas Y axis denotes the No of Infected Nodes victimization each the Intrusion detection Multipath Routing and our projected weighted vote primarily based Trust Management Technique. once the amount of nodes will increase the no of Infected additionally gets enlarged. Figure four shows the effectiveness of Nn of Infected over totally different variety of nodes than existing Intrusion detection Multipath Routing and our projected weighted vote primarily based Trust Management. Weighted vote primarily based Trust Management achieves half-hour to five hundredth additional No of Infected Nodes in comparison with existing schemes.

V. CONCLUSION

During this paper we tend to performed a trade-off analysis of energy consumption vs. QoS gain in responsibleness, timeliness, and security for redundancy management of clustered heterogeneous wireless sensing element networks utilizing weighted vote primarily based trust management to answer user queries. Finally, we tend to applied our analysis results to {the style|the planning|the look} of a Weighted vote base Trust Management formula to spot and apply the most effective design parameter settings in Ns2. we tend to enforced the projected theme, and conducted comprehensive performance analysis and analysis, that showed its potency and blessings over existing schemes.

VI. REFERENCES

[1] Carol J Fung Jie Zhang Issam Aib Raouf Boutaba "Robust and ascendible Trust Management for cooperative Intrusion Detection".

[2] Carol J Fung Jie Zhang Raouf Boutaba "Effective Acquaintance Management for Collaborative Intrusion Detection Networks".

[3] Ramaprabhu Janakiraman, Marcel Waldvogel, Qi Zhang, "A peer-to-peer approach to network intrusion detection and prevention".

[4] Todd Sproull and John Lockwood," Distributed Intrusion hindrance in Active and extensile Networks".

[5] Yan Lindsay Sun, Zhu Han, Wei dynasty Yu and K. J. Ray Liu "A Trust analysis Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks".

[6] Chenfeng Vincent Zhou, Shanika Karunasekera and Saint Christopher LE," A Peer-to-Peer cooperative Intrusion Detection System".

[7] Ioannis Krontiris, Tassos Dimitriou and Felix C. Freiling, "Towards Intrusion Detection in Wireless sensing element Networks".

[8] Ana Paula R. district attorney timber Marcelo H.T. Martins Bruno P.S. Rocha, " localized Intrusion Detection in Wireless sensing element Networks".

[9] Bo sun and Lawrence dramatist, Yang Xiao, Sghaier Guizani, "Intrusion detection techniques in mobile impromptu and wireless sensing element networks".

[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] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE* Trans. MobileComput., vol. 3, no. 4, pp. 366–379, 2004.

[12] 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

[13] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *IEEE* Wireless Commun. *Mag.*, vol. 14, no. 5, pp. 560–563, 2007.

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

[15] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," IEEE Trans. Reliab., vol. 59, no. 1, pp. 231–241, 2010.

[16] 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

[17] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," *J. Netw.* Comput. Appl., vol. 33, no. 4, pp. 422–432, 2010

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

[19] 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.

[20] 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.

[21] Jin-Hee Cho, Ing-Ray Chen: Performance analysis of gradable cluster key management integrated withadaptive intrusion detection in mobile impromptu networks. Perform. Eval. 68(1): 58-75 (2011)

[22] Ing-Ray Chen, Anh Phan Albert Speer, Mohamed Eltoweissy: adaptive Fault-Tolerant QoS managementAlgorithmsfor increasing System time period of Query-Based Wireless detector Networks. IEEE Trans. Dependable Sec. Comput. 8(2): 161-176 (2011)

[23] Fenye Bao, Ing-Ray Chen, Moonjeong Chang Jiang, Jin-Hee Cho: Trust-Based Intrusion Detection in Wirelessdetector Networks. Interstate Commerce Commission 2011: 1-6

[24] Yinan Li, Ing-Ray Chen: gradable Agent-Based Secure Multicast for Wireless Mesh Networks. Interstate Commerce Commission 2011: 1-6

[25] Ing-Ray Chen, Anh Ngoc Albert Speer, MohamedEltoweissy:Dynamic adaptive redundancy for quality-of-service management in wireless detector networks. IPDPS 2009: 1-8

[26] Anh Phan Albert Speer, Ing-Ray Chen: result of redundancy on the mean solar time to failure of wirelessdetector networks. Concurrency and Computation: follow and knowledge 19(8): 1119-1128 (2007)

[27] Anh Phan Albert Speer, Ing-Ray Chen: result of Redundancy on mean solar time to Failure of Wirelessdetector Networks. AINA (2) 2006: 373-382

[28] Anh Phan Albert Speer, Ing-Ray Chen: On best Path and supply Redundancy for Achieving QoS andincreasing time period of Query-Based Wireless detector Networks. MASCOTS 2006: 51-60

[29] Hamid Al-Hamadi, Ing-Ray Chen: Energy vs. QoS trade-off Analysis of Multipath Routing Protocols for Intrusion Tolerance in Heterogeneous Wireless detector Networks. ISPA 2012: 387-394