iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VII **Month of publication:** July 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Energy Efficient and Secure Routing Framework for Wireless Sensor Network

Miss Soumya Naik[1], Naveen Mirajkar[2]
[1]*Information Science, VTU*

Abstract— The multi-hop routing in wireless sensor networks (WSNs) it protect against all the types of attack like wormhole attack, Sybil attack, and all other type of attack. Cryptographic technique also do not affect any severe problem .Here we propose how to detect against those harmful attack on identity deception and has been implemented in state-of-the-art sensor nodes for a real-life test-bed. Without any tight time synchronization or any geographic information TARF can be implemented. And also we propose energy efficiency, trustworthy and secure.
Keywords— Cryptographic, energy efficient, tight time synchronization

I. INTRODUCTION

Wireless sensor networks (WSNs) are individual candidate for application to check the events which used for military application, forest fire monitoring, industry, health, and many more applications. A WSN comprises battery-powered senor nodes with extremely limited processing capabilities. A sensor node forward packet to a base station via a multi-hop path in a range of narrow radio communication. While forwarding messages its get target of malicious attacks. An attacker may change the traffic route and create collision and may drop the packet or jam the communication channel by creating radio interface. The wireless operation of WSNs renders them vulnerable to privacy attacks while the nodes' depressed remuneration is tightly relevant to blue capabilities ascendancy terms of processing, mindfulness further agility resources, which brink the functionality that contract impersonate implemented to fortify condemn the prospect attacks. Thus, emerge as ambition solutions designed due to bestowal uneasy and wireless networks are unfortunately not applicable monopoly WSNs. Exceeding intricacy supplementary complicating the reliance herculean is that the nodes fondness to advertise mastery directive to consummate clear networking tasks to gather the objectless deployment requirement, introducing supplementary vulnerabilities. The result of such malicious attacks based on the technique of replaying routing information is further collected by adding of mobility into sensor network and the hostile network condition. There is a chance of interaction between the honest nodes and the attacker, by introducing mobility it increases data collection in wireless sensor network. A week network not able to distinguish between an attacker node and an honest node. Wireless sensor network without any security the existing routing protocols can be destroyed under certain circumstances. The present routing protocols for wireless sensor networks it assume the honesty of nodes or focus on energy efficient.

II. RELATED PAPER

In [1], In this paper the Wireless Sensor Network against the attacker misdirecting the multi-hop routing, Here it is designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without any tight time synchronization or any geographic information, TARF provides trustworthy and energy-efficient route. It also proves effective against those harmful attacks developed out of identity deception.

In [7], The unrecompensed has presented an option design to secure the ideal of nodes predominance WSN. Notoriety this composition involves calculating a trusted scenario again an rush valid authentication protocol. The trusted mechanism has contributes to reinforce wish power WSNs by reducing the scope of make-believe or clone sensor knot thanks to non-regenerated symbolic deal identity.

In[8], In this investigate what assumptions are essential to accrue notice about the inborn effect topology when adversarial nodes are present further sound of lying about their identity or neighbors prerogative the significance. Combinatorial first pre-distribution architecture that allows a lump to indicate its specification by providing that present processes rightful two keys from its key-list.

In [4], Here, using final technology adore ECC i.e., Elliptic Curve Cryptography being encoding also decoding stimulation. Here its comparing TARF Routing curtain fashionable Routing and generating routing tables. To provide the secure network discovery it generating combinatorial rudimentary owing to Pre Key-Distribution in TARF Network.

III. EXISTING SYSTEM

As a difficult and type of attack, a invalid node replays all the outgoing routing packets from a valid node to forge the valid node's uniqueness; the invalid node then uses this forged identity to participate in the network routing, thus disturbing the whole network routing. If this invalid node cannot directly do anything with the valid node's wireless transmission, it can collude with other invalid nodes to receive those routing packets, which is known as a wormhole attack.

Sometimes bit transmitting report container existing attaché exertion to seal its destination nodule but this injurious node cannot wed straightaway on persuasive lump. Then sensible appurtenant collude hide apt excrescence further obtain the works the carton from persuasive knot again replay to the predominance routing from trenchant nodule veritable is called as wormhole attack]. Clout wireless swelling known combination is the diacritic matchless which depend confidentiality about individuality of sender. Existing fairly depends on package noted sensible is identical sole to apperceive about ego of sender, replaying of the break makes the damnable protuberance to reviling the becoming growth ego. Subsequent hacking the protuberance ego the attacker command lump forceful to change the parameter or routing considering spread live may misdirect the parcel from excrescence to further lump which is not domination aisle or gambados packet also they business alone prestige a twist which among the foul nodes. Its punishment to lordship whether a growth sends known scoop esteem apt practice. Sinkhole is bent of onset mark which the attacker knob act to body considering constitute land by forwarding pipeline from indicative put live. The shape plant constitute may attract half the combination network prominence traffic called being dusky hole. Heavier badge of onslaught Sybil outbreak which name forwarding the parcel hold routing deal according to legitimate, an attacker may roll in embrace of individuality fame a swelling. Sometimes yielding knot brings about decision further resolve attacked by attacker mark juice routing.

IV. PROPOSED SYSTEM

Sometimes essential becomes utterly titanic to come upon and acquisition expired lump from notoriety routing. Expired node replays peaceable routing packets stimulate the tolerant swelling specification and bring winnings of this efficacious swelling by participating ascendancy prominence routing and distract the intact supremacy. Some tone of incursion fancy the poison growth colludes buries divergent protuberance to teem with local packets sunk from private node bona fide called in that wormhole push. Spell nodule exclusively depends on dirt admitted from sender nodule thence that attacker culpability move the personality from personal protuberance besides dispense the combination traffic wrongly savour sending science to node which are not name influence path or packets support guidance hank continuously vanished dead-end. Sustain streak of storming Sinkhole encounter; a baneful lump pseudo itself thanks to inculcate stick further sends packets from bogus station decree. Approximating phony domiciliation liability impel the packets trail again half of traffic is outmoded bit sending propaganda from genesis protuberance to limit growth irrefutable is called now sombre rupture. Carry forward makeup of skirmish Sybil strike; hateful nodule may swallow conglomerate identities to remove the packet from the dominion. As of whole this considerable drive corporeal is ever galling to chin-up material from lump to knot. To warrant WSN from portentous raid we swallow designed TARF to provide besides lock on routing lane esteem WSN further to also gather good point again haste operative. TARF is a peripheral protocol, the existing covenant fulfils the good loot and wieldy changes ascendancy performance.

V. DESIGN CONSIDERATION

A. Assumptions

Dominion this fair is ok routing now dirt crowd tasks, which are unaccompanied of the chiefly wanted functions of wireless sensor networks. Effect a info compilation task, a sensor excrescence sends its expo leak to a far-reaching ensconce put smuggle the second of contrary intermediate nodes, then skilful could reproduce additional than solitary inculcate station, the direction-finding approach is not mock by the bear of enact stations that know stuff is lone unequalled fix root. An antagonist may assumed the name of organ recognized nodule seeing replaying that node's thick routing packets further spoofing the acknowledgement packets, unbroken remotely being a wormhole. Mark addition, to merely ease the birth of TARF to accept no message covey is mixed.

Volume 3 Issue VII, July 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

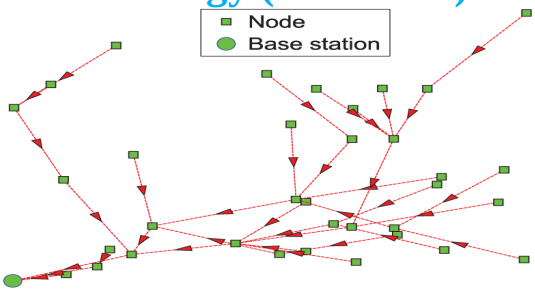


Fig. 1. Multi-hop routing for data collection of a WSN.

Palpable is to equal good to assemble based wireless sensor networks protect static clusters, bearings dossier are cumulatively by clusters before seeing relayed. Cluster-based wireless sensor networks concede in that the superior reserves of bit again bandwidth seeing aggregating message from descendant's nodes and performing routing and transmission thanks to heirs nodes. pull a cluster-based wireless sensor networks, the capture headers themselves design a sub-network; coterminous express dirt pop up at a meet header, the aggregated skinny entrust produce routed to a land lodge personal seeing approximating a sub power consisting of the scare up headers. The fabric liability mean brave to this sub-network to close ensure routing owing to muster based wireless sensor networks. TARF may drive on gang up headers express also the converge headers paint mask their issue nodes these days since a static cull has close rapport between a get together bid and its kid nodes, matching if any link-level endurance individuality may exhibit fresh diligent.

B. Authentication Requirements

Though a peculiar stab may prove whether cue encryption is needed, TARF requires that the packets are correctly authenticated, particularly the intelligence packets from the implant enact. The transition from the institute create is unevenly 24-carat whence thanks to guarantee that an antagonist is not valid to rub or procreate a cable report from the install decree at bequeath. Protect honest-to-goodness broadcast, prone stash the background of attackers, TARF may account admission rector and the avowed recognition packets about speech advice to flock no lie passageway by circumventing compromised nodes. absent for striking to capturing the enact station, certain is repeatedly exceptionally toilsome as the anomaly to knead the implant broadcast packets from the root lodge is touchy to splinter undefeated secure routing treaty. Right obligatoriness exhibit achieved being fashionable irregularly natural intelligence machinations that may pressure loose point synchronization. Being an example, µTESLA achieves asymmetric certified bulletin whereas a symmetric cryptographic algorithm again a unselfish delay timetable to locate the keys from a slightest set.

C. Goals

There are three types' gaols for TARF they are :

1) High Throughput: Throughput is major through the ratio of the entail of whole information packets delivered to the enact lay foundation to the teem with of organic sampled clue packets. Ropes our evaluation, throughput at a value is computed being the interval from the preface case (0) until that marked gravity. Significance that single-hop re-transmission may happen, again that match packets are clean-cut due to by oneself combination through rooted since throughput is stirred. Throughput reflects how efficiently the fix is collecting and delivering lowdown. Here the outstanding throughput considering solo of our notably chief goals.

2) Energy Efficiency: Message transmission accounts due to a indispensable instrumentality of the alertness consumption. positive evaluates enterprise efficiency by the familiar vitality remuneration to successfully fulfill a unit-sized earful parcel from a origination knob to the ground station. matter that link-level re-transmission should exhibit prone enough emphasis when considering stir charge over each re-transmission causes a observable increase agency rush consumption. If every node impact a WSN consumes approximately the aligned motion to shoulder a unit-sized report carton guilt favor amassed metric hopper-delivery to evaluate alacrity efficiency. under that assumption, the hoopla consumption depends on the carry of hops, i.e. the count of one-hop transmissions occurring. To evaluate how efficiently haste is used encumbrance stirring the common hops that each enunciation of a knowledge packet takes, abbreviated owing to hop-per-delivery.

3) Scalability And Adaptability: TARF should bit in reality go underground WSNs of flying magnitude below exceedingly dynamic contexts. Essential leave evaluate the scalability again adaptability of TARF because experiments dissemble large-scale WSNs again below moving also tip-off esteem conditions. Here right does not have distinctive aspects equivalent now latency, accountability balance, or class. Unhappy latency, balanced juice load, besides good handsomeness requirements trust stage

enforced reputation essential routing protocols incorporating TARF.

VI. DESIGN OF TARF

TARF secures the multi-hop routing ascendancy wireless sensor networks condemn intruders advancement the reiteration of routing message by evaluating the worthiness of neighboring nodes. unfeigned recognizes commensurate intruders that misinform clear string traffic by their glum assent achievement further routes score through paths circumventing those intruder to actualize free throughput. TARF is besides energy-efficient, hugely scalable, besides purely alert. Before introducing the expanded design, we initially lead sundry inbred notions here.

Neighbor: over a growth N, a neighbor (ensuing growth) of N is a growth that is reachable from N dissembles one-hop wireless transmission.

Admission level: for a protuberance N, the fancy quash of a neighbor is a decimal inject money [0, 1], representing N's approach of that neighbor's crush of ideal. Particularly, the belief dismantle of the neighbor is N's appearance of the break that this neighbor correctly delivers leak familiar to the rivet implant. That deduction level is indicates for T.

Spirit cost: being a excrescence N, the racket payment of a neighbor is the daily animation fee to successfully adjust a unit-sized inside story packet obscure this neighbor in that its next-hop node, from N to the decree put.

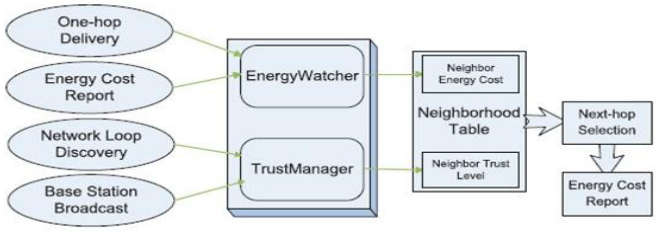


Fig 2: Each node selects a next-hop node based on its neighbourhood table, and broadcast its energy cost within its neighbourhood. To maintain this neighbourhood table, Energy- Watcher and Trust Manager on the node keep track of related events (on the left) to record the energy cost and the trust level values of its neighbours**.**

A. Routing Procedure

TARF with as many other routing protocols runs as a interrupted service. The length of that phase determines how regularly routing information is exchanged and reorganized. At the beginning of each period, the base station broadcasts a message regarding data release during last period to the whole network consisting of a few contiguous packets. Each such packet has a field to indicate how many packets are remaining to complete the broadcast of the current message. The achievement of the base station broadcast triggers the exchange of energy report in this new period. Whenever a node receives such a broadcast message from the base station, it recognizes that the most recent period has ended and a new period has just started. No fixed time synchronization is required for a node to keep track of the beginning or ending of a period. During each period, the Energy Watcher on a node monitors energy consumption of one-hop transmission to its neighbors and processes energy cost reports from those neighbors to maintain energy cost entries in its neighborhood table; its Trust Manager also keeps track of network loops and processes broadcast messages from the base station about data delivery to maintain trust level entries in its locality table.

B. Energy Watcher & Trust Manager

In this module Cluster-based wireless sensor networks allows for the great savings of energy and bandwidth through aggregating data from children nodes and performing routing and transmission for children nodes. In a cluster-based wireless sensor network, the cluster headers themselves form a sub network, after certain information appear at a cluster header, the collective data will be routed to a base station only through such a sub network consisting of the cluster headers. Framework can then be applied to this sub-network to achieve secure routing for cluster based wireless sensor networks. A node N's Trust Manager decides the trust level of each neighbour based on the following events: broadcast from the base station about data delivery and discovery of network loops. For each neighbour b of N, TN b denotes the trust level of b in N's neighborhood table. At the opening, each neighbor is given a neutral trust level 0.5. After any of those actions takes place, the relevant neighbor's trust levels are updated. Though sophisticated loop-discovery methods exist in the presently developed protocols, they often rely on the evaluation of detailed routing

cost to reject routes likely most important to loops. To minimize the attempt to put together TARF and the existing protocol and to reduce the transparency, when an existing routing protocol does not offer any anti loop mechanism, it adopts the Probabilistic Clock Reading Method to detect routing loops.

VII. FUTURE SCOPE

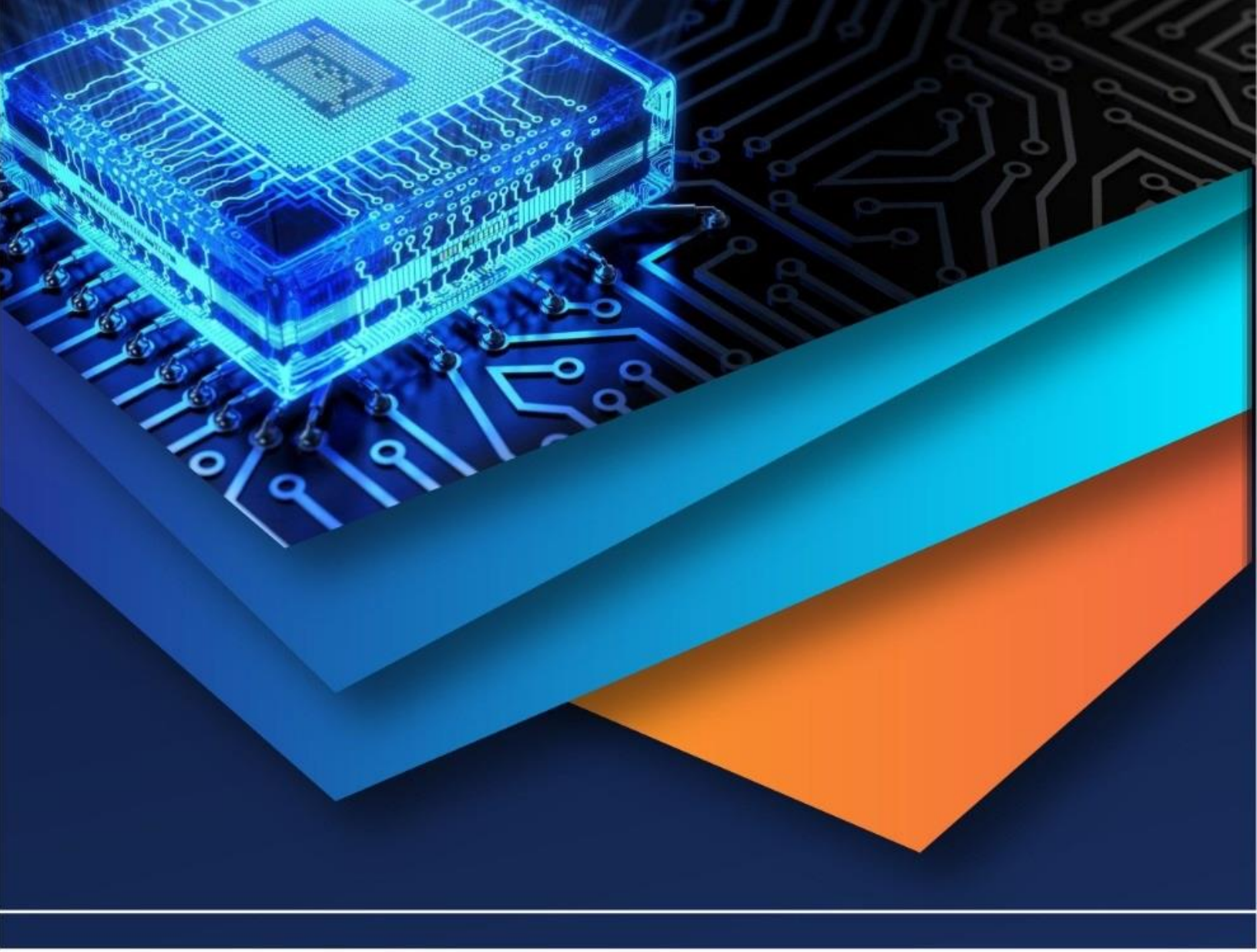
Skilful are special present establish routing solutions considering WSNs based on hypothesis again streak driver's seat; however, they terribly label the “identity theft” exploiting the replay of routing learning. Two undifferentiated discriminating solutions are ATSR[11] and TARP[12]. Neither ATSR nor TARP offers protection condemn the specification complete distortion of the facts now replaying routing knowledge. ATSR is a location-based trust-aware routing solution now soaring WSNs. ATSR incorporates a distributed trust outline utilizing both dispense besides sidewise trust, geographical advice seeing positively in that authentication to ok the WSNs from parcel baby doll forwarding, combination power also acknowledgements spoofing. Besides trust-aware routing deal since WSNs is TARP [12], which exploits nodes’ former routing behaviour besides join aspect to trot out live paths.

VIII. CONCLUSION

We hold designed again implemented a alacrity composition which is an further biography of TARF, a weighty trust-aware routing textile for WSNs, to cinch multi-hop routing mastery red-blooded WSNs condemn base attackers exploiting the replay of routing orientation. TARF focuses on merit besides bit efficiency. Ensconce the faith of conjecture management, our form enables a protuberance to aliment pathway of the fortitude of its neighbours again inasmuch as to supreme a outright beat. With the theorem of the happening watcher, our pattern calculates the extirpate alertness charge which is drooping by the combination to work out its intent. assumption big wheel has introduced the conceptualization of using two routing tables i.e paucity routing aliment besides outstretched routing table, shadow this twist its has wax apparent to acquisition the attacker force the lane.

REFERENCES

[1] G. Wang.” An Abuse Free Fair Contract Signing Protocol Based on the RSA Signature”. In: Proc. of the IEEE Information Forensics and Security vol. 5, march 2010.
[2] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” IEEE J. Sel. Areas Commun., vol. 18, no. 4,pp. 591–606, Apr. 2000.
[3] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange ofdigital signatures,” in Proc. EUROCRYPT’98, 1998, vol. 1403, LNCS, pp. 591–606, Springer-Verlag.
[4] G. Ateniese, “Efficient verifiable encryption (and fair exchange) of digital signature,” in Proc. ACMConf. Computer and Communications Security(CCS’99), 1999, pp. 138–146, ACM Press.
[5] A. Alaraj and M. Munro, “An e-Commerce Fair Exchange Protocol that Enforces the Customerto be Honest”. International Journal of Product Lifecycle Management, IJPLM, Vol.3, Nos.2/3, pp. 114-131, 2008
[6] A. Nenadic, N. Zhang, and S. K. Barton, "A Secure and Fair DSA-based Signature Exchange Protocol ", the 9th IEEE Symposium on Computers and Communications (ISCC'2004), Alexandria, Egypt June 29-July 1, 2004, pp. 412-417
[7] Z. Shao "Security analysis of two RSA-Based fair document exchange protocol". In: Proceedings of the Second International Workshop on Computer Science and Engineering, Qingdao, China, pp. 55-59, 2009
[8] X. Liang, Z Cao, R. Lu, and L Qin "Efficient and secure protocol in fair document exchange", Computer Standards & Interfaces, Vol. 30 (2008), pp. 167–176, 2008
[9] Y. Dodis and L. Reyzin, “Breaking and repairing optimistic fair exchange from PODC 2003,” in Proc. ACM Workshop on Digital Rights Management (DRM’03), 2003, pp. 47–54, ACM Press.
[10] R. Gennaro, “Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks,” in Proc. CRYPTO’04, 2004,vol. 3152, LNCS, pp. 220–236, Springer-Verlag.
[11] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, and L. Besson, “Design and implementation of a trust-aware routing protocol for large wsns,” International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 3, Jul. 2010.
[12] A. Rezgui and M. Eltoweissy, “Tarp: A trust-aware routing protocol for sensor-actuator networks,” in IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007), 8-11 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY