Enhanced Trust Aware Routing Framework against Sinkhole Attacks in Wireless Sensor Networks

Pushkar A. Chavan, Rashmi D. Aher, Kamlesh V. Khairnar, Hemant D. Sonawane

***Abstract*— The multi-hop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the WSNs against adversaries misdirecting the multi-hop routing, we have designed and implemented ETARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, ETARF provides trustworthy and energy-efficient route. Most importantly, ETARF proves effective against those harmful attacks developed out of identity deception; the resilience of ETARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. Further, we have implemented a low-overhead ETARF module in Tiny OS; as demonstrated, this implementation can be incorporated into existing routing protocols with the least effort. Based on ETARF, we also demonstrated a proof-of-concept mobile target detection application that functions well against an anti-detection mechanism.**

***Index Terms*— Attacks, Routing, WSN, ETARF,Sinkhole.**

I. INTRODUCTION

Wireless sensor networks (WSNs) are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. A WSN comprises battery-powered senor nodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multi-hop path. However, the multi hop routing of WSNs often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference. This paper focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception, the adversary is capable of launching harmful and hard-to-detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks and Sybil attacks.

Manuscript received December 31, 2014.
Pushkar A. Chavan, Comp Dept. BVCOERI, Nashik, India.
Rashmi D. Aher, Comp Dept. BVCOERI, Nashik, India.
Kamlesh V. Khairnar, Comp Dept. BVCOERI, Nashik, India.
Hemant D. Sonawane, Comp Dept. BVCOERI, Nashik, India.

As a harmful and easy-to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity the malicious node then uses this forged identity to participate in the network routing, thus disrupting. Those routing packets, including their original headers, are replayed without any modification. Even if this malicious node cannot directly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets and replay them somewhere far away from the original valid node, which is known as a wormhole attack. Since a node in a WSN usually relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a "black hole". This same technique can be employed to conduct another strong form of attack :

A. Sybil attack

Through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks. The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into WSNs and the hostile network condition. Though mobility is introduced into WSNs for efficient data collection various applications it greatly increases the chance of interaction between the honest nodes and the attackers. Additionally, a poor network connection causes much difficulty in distinguishing between an attacker and a honest node with transient failure. Without proper protection, WSNs with existing routing protocols can be completely devastated under certain circumstances. In an emergent sensing application through WSNs, saving the network from being devastated becomes crucial to the success of the application. Unfortunately, most existing routing protocols for WSNs either assume the honesty of nodes or

focus on energy efficiency, or attempt to exclude unauthorized participation by encrypting data and authenticating packets. Examples of these encryption and authentication schemes for WSNs include Tiny Sec, Spins, Tiny PK, and Tiny ECC. Admittedly, it is important to consider efficient energy use for battery powered sensor nodes and the robustness of routing under topological changes as well as common faults in a wild environment. However, it is also critical to incorporate security as one of the most important goals; meanwhile, even with perfect encryption and authentication, by replaying routing information, a malicious node can still participate in the network using another valid node's identity.

The gossiping-based routing protocols offer certain protection against attackers by selecting random neighbors to forward packets, but at a price of considerable overhead in propagation time and energy use. In addition to the cryptographic methods, trust and reputation management has been employed in generic ad hoc networks and WSNs to secure routing protocols basically, a system of trust and reputation management assigns each node a trust value according to its past performance in routing. Then such trust values are used to help decide a secure and efficient route. However, the proposed trust and reputation management systems for generic ad hoc networks target only relatively powerful hardware platforms such as laptops and smart phones. Those systems cannot be applied to SNs due to the excessive overhead for source-constrained sensor nodes powered by batteries. s far as WSNs are concerned, secure routing solutions based on trust and reputation management rarely address he identity deception through replaying routing information. The countermeasures proposed so are strongly depends on either right time synchronization or known geographic information while their effectiveness against attacks exploiting the replay of routing information has not been examined yet. At this point, to protect WSNs from the harmful attacks exploiting the replay of routing information, we have designed and implemented a robust trust-aware routing framework, ETARF, to secure routing solutions in wireless sensor networks. Based on the unique characteristics of resource constrained WSN, the design of ETARF centers on trustworthiness and energy efficiency.

Though ETARF can be developed into a complete and independent routing protocol, the purpose is to allow existing routing protocols to incorporate our implementation of ETARF with the least effort and thus producing a secure and efficient fully-functional protocol. Unlike other security measures, ETARF requires neither tight time synchronization\ nor known geographic information. Most importantly, ETARF proves resilient under various attacks exploiting the replay of routing information, which is not achieved by previous security protocols. Even under strong attacks such as sinkhole attacks, wormhole attacks as well as Sybil attacks, and hostile mobile network condition, ETARF demonstrates steady improvement in network performance. The effectiveness of ETARF is verified through extensive evaluation with simulation and empirical experiments on large-scale WSNs.

Finally, we have implemented a ready-to-use ETARF module with low overhead, which as demonstrated can be integrated into existing routing protocols with ease; the demonstration of a proof-of-concept mobile target detection program indicates the potential of ETARF in WSN applications. We start by stating the design considerations of ETARF. Then we elaborate the design of ETARF including the routing procedure as well s the energy Watcher and Trust Manager Components. We present the simulation results of ETARF against various attacks through replaying routing information in static, mobile and RF-shielding conditions further presents the implementation of ETARF, empirical evaluation at a large sensor network and a resilient proof-of-concept mobile target detection application based on ETARF.

II. OBJECTIVES

ETARF mainly guards a WSN against the attacks misdirecting the multi-hop routing, especially those based on identity theft through replaying the routing information. This paper does not address the denial of service (DoS) attacks, where an attacker intends to damage the network by exhausting its resource. For instance, we do not address the DoS attack of congesting the network by replaying numerous packets or physically jamming the network. ETARF aims to achieve the following desirable properties:

High Throughput is defined as the ratio of the number of all data packets delivered to the base station to the number of all sampled data packets. In our evaluation, throughput at a moment is computed over the period from the beginning time (0) until that particular moment. Note that single-hop re-transmission may happen, and that duplicate packets are considered as one packet as far as throughput is concerned. Through-put reflects how efficiently the network is collecting and delivering data. Here we regard high throughput as one of our most important goals.

Energy Efficiency Data transmission accounts for a major portion of the energy consumption. We valuate energy efficiency by the average energy cost to successfully deliver a unit-sized data packet from a source node to the base station. Note that link-level re-transmission should be given enough attention when considering energy cost since each re-transmission causes a noticeable increase in energy consumption. If every node in a WSN consumes approximately the same energy to transmit a unit-sized data packet, we can use another metric hop-per-delivery to evaluate energy efficiency. Under that assumption, the energy consumption depends on the number of hops, i.e. the number of one-hop transmissions occurring. To evaluate how efficiently energy is used, we can measure the average hops that each delivery of a data packet takes, abbreviated as hop-per-delivery.

Scalability & Adaptability ETARF should work well with WSNs of large magnitude under highly dynamic contexts. We will evaluate the scalability and adaptability of ETARF through experiments with large-scale WSNs and under mobile and hash network conditions. Here we do not include other aspects such as latency, load balance, or fairness. Low latency, balanced network load, and good fairness requirements can be enforced in specific routing protocols incorporating ETARF.

III. EXISTING SYSTEM

In Existing system, when the file send from base station in that situation hackers aggravated network conditions. A traditional cryptographic techniques effort does not address the severe problems. That time the file could be affected by hackers. So, the network will be damaged. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference.

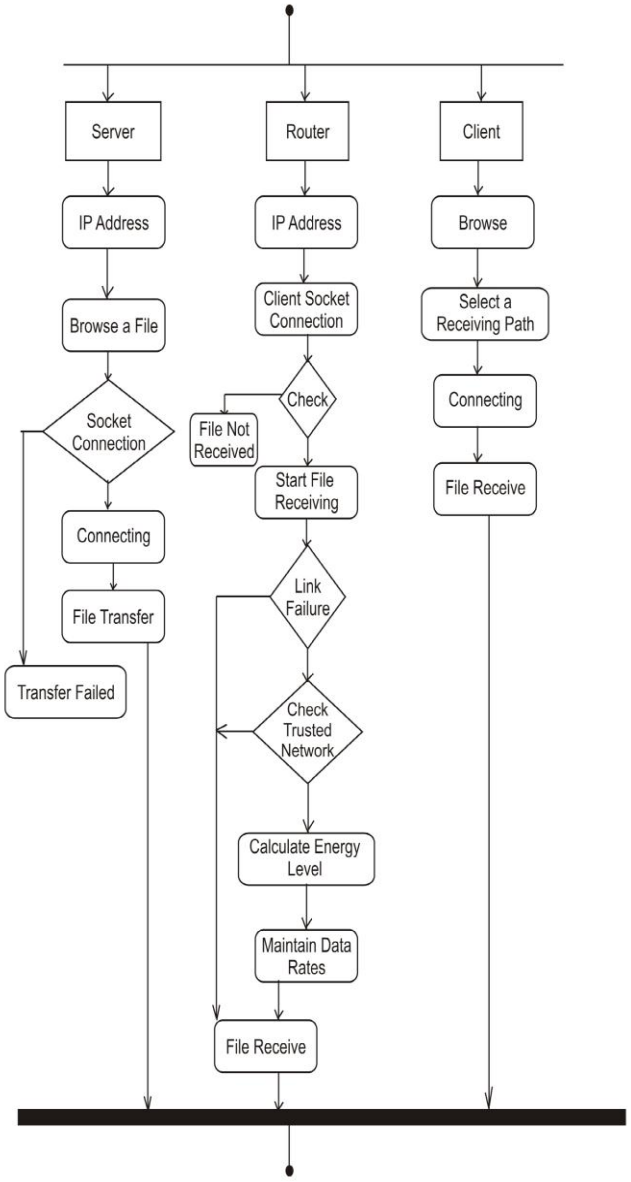
IV. PROPOSED SYSTEM

In Proposed System, focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception the adversary is capable of launching harmful and hard to detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks, and Sybil attacks. ETARF, as with many other routing protocols, runs as a periodic service. The length of that period determines how frequently routing information is exchanged and updated. At the beginning of each period, the base station broadcasts a message about data delivery during last period to the whole network consisting of a few contiguous packets (one packet may not hold all the information). Each such packet has a field to indicate how many packets are remaining to complete the broadcast of the current message.

The completion 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 knows that the most recent period has ended and a new period has just started. No tight 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 neighborhood table. To maintain the stability of its routing path, a node may retain the same next-hop node until the next fresh broadcast message from the base station occurs. Meanwhile, to reduce traffic, its energy cost report could be configured to not occur again until the next fresh broadcast message from the base station.

If a node does not change its next-hop node selection until the next broadcast message from the base station that guarantees all paths to be loop-free, as can be deducted from the procedure of next-hop node selection. However, as noted in our experiments, that would lead to slow improvement in routing paths. Therefore, we allow a node to change its next-hop selection in a period when its current next-hop node performs the task of receiving and delivering data poorly. Next, we introduce the structure and exchange of routing information as well as how nodes make routing decisions in ETARF.

V. ACTIVITY FLOW



VI. ALGORITHM USED

A. Routing the Network

In this module, the networks embedded on the physical fiber topology. However, assessing the performance reliability achieved independent logical links can share the same physical link, which can lead to correlated failures. Mainly, we focus on assessing the reliability of energy level and trusted network.

B. Transfer File

In this module, Analysis the Shortest Path algorithm independently routes each logical link on a physical path with the minimum number of hops in trusted network basis. Since we are assuming that every physical link fails with the same probability, the failure probability of path is minimized when it is routed over the shortest path. Hence, under the algorithm Shortest Path, each light- path greedily takes the most reliable route and transfers the file.

C. Sinkhole Attacks

- Prevent the base station from obtaining complete and correct sensing data
- Particularly severe for wireless sensor networks
- Some secure or geographic based routing protocols resist to the sinkhole attacks in certain level
- Many current routing protocols in sensor networks are susceptible to the sinkhole attack
- Set of sensor nodes

a) Continuously monitor their surroundings

b) Forward the sensing data to a sink node

- Many-to-one Communication

a) Vulnerable to the sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information

b) Alters the data passing through it or performs selective forwarding.

D. Energy Watcher & Trust Manager

In this module Cluster-based WSNs 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 WSN, the cluster headers themselves form a sub-network, after certain data reach a cluster header, the aggregated data will be routed to a base station only through such a sub-network consisting of the cluster headers. Our framework can then be applied to this sub-network to achieve secure routing for cluster based WSNs.

VII. CONCLUSION

Our system designed and implemented ETARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. ETARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment. With the idea of trust management, ETARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. Unlike previous efforts at secure routing for WSNs, ETARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information. The resilience and scalability of ETARF is proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks. Our system implemented a ready-to-use Tiny OS module of ETARF with low overhead; as demonstrated in the paper, this ETARF module can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully-functional protocols. Finally, we demonstrate a proof-of-concept mobile target detection application that is built on top of ETARF and is resilient in the presence of an anti-detection mechanism; that indicates the potential of ETARF in WSN applications.

ACKNOWLEDGMENT

It is my pleasure to express my knowledge to my respected sir Prof. H. D. Sonawane, Computer Engineering, BVCOE&RI, Nashik for his valuable guidance, inspiration and continues support. This paper could not be success without ETARF analysis done which help to understand the necessity for this paper.

REFERENCES

[1] Guoxing Zhan, Weisong Shi, and Julia Deng, TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks, Conference on Wireless Sensor Networks, Coimbra, Portugal, Feb. 17-19, 2010.

[2] Al-Karaki, J., Kamal, A.: Routing techniques in wireless sensor networks: a survey. IEEE Wireless Communications 11(6), 6–28 (2004).

[3] B. Sai Pragna, M. Shakeel Ahmed, B.Sai Manogna, Performance Analysis of Trust-Aware Routing Framework for Wireless Mesh Networks, IJMER Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2867-2871.

[4] Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis, DESIGN AND IMPLEMENTATION OF A TRUST-AWARE ROUTING PROTOCOL FOR LARGE WSN, IJNSA, Vol.2, No.3, July 2010.

[5] Ms. Dipali G. Dikondwar, Prof. R. K. Krishna, Performance Analysis of Implementation of Trust Aware Routing Framework (TARF) for Large Scale WSNs, IJRICCE Vol. 1, Issue 5, July 2013.