

# The Insecurity of Time-of-Arrival Distance-Ranging in IEEE 802.11 Wireless Networks

Steve Glass<sup>\*†</sup>, Vallipuram Muthukumarasamy<sup>\*†</sup> and Marius Portmann<sup>\*‡</sup>

<sup>\*</sup>NICTA, Queensland Research Laboratory, Brisbane, Australia

<sup>†</sup>School of Information and Communications Technology, Griffith University, Gold Coast, Australia

<sup>‡</sup>School of Information Technology & Electrical Engineering, University of Queensland, Brisbane, Australia

Email: s.glass@nicta.com.au, v.muthu@griffith.edu.au, marius@itee.uq.edu.au

**Abstract**—Two-way Time-of-Arrival (TOA) distance-ranging is well-suited for use in IEEE 802.11 MANETs and wireless mesh networks because it is simple, efficient and does not require precise time synchronization between network stations. Despite its utility we show that this distance-ranging procedure is completely insecure and demonstrate how it can be subverted by a simple but highly effective attack. This attack allows the adversary comprehensive and fine-grained control over the distance reported by the procedure. Such adversaries can appear to be either much further away or much closer than they are in reality. We demonstrate the attack experimentally and also show how it can be implemented using ordinary wireless network interfaces. Finally, the necessary and sufficient conditions for the secure use of two-way TOA distance-ranging procedure in IEEE 802.11 wireless networks are identified.

**Index Terms**—Computer network security; Wireless LAN; Delay estimation; Distance measurement; Position measurement

## I. INTRODUCTION

In wireless networks an effective distance-ranging procedure is a very useful security primitive. Such distance-ranging procedures can be used to implement station localization, location-based authentication and assist in the detection and prevention of routing wormholes. Time of arrival (TOA) distance-ranging is simple and efficient and needs no advance preparation such as the surveys required by received signal-strength approaches. TOA distance-ranging is, therefore, well-suited to dynamic, mobile networks such as MANETs and Wireless Mesh Networks (WMNs).

The TOA ranging procedure measures the time taken for a radio wave to propagate from the sending station to the receiving station. The propagation delay is directly proportional to the distance travelled by the radio wave. Given the velocity of the radio wave through the air (in  $1\mu\text{s}$  a radio wave traverses almost 300m) a distance estimate is easily computed. The simple TOA procedure requires that both sender and receiver have precisely synchronized clocks and that the sender attaches a timestamp to the outgoing frame. The receiver takes the difference between the timestamp and clock from which it can compute the distance estimate. In many wireless networks the clock synchronization insufficiently precise to allow for the simple TOA distance-ranging. The two-way TOA distance-ranging procedure avoids this requirement by measuring the time taken for a round-trip message exchange such as DATA/ACK, RTS/CTS or Probe/Response [1]. This

approach is well-represented in the literature with several researchers claiming to be able to locate IEEE 802.11 network stations with an accuracy of 5 meters or better [2]–[6].

## A. Two-Way TOA Distance-Ranging in IEEE 802.11

To illustrate the two-way TOA procedure we use the example of two network stations  $A$  and  $B$  in which  $A$  is estimating the distance to  $B$ . Figure 1 gives a timing diagram for a simple DATA/ACK exchange in which  $A$  sends a 128 octet data frame to  $B$  at 5.5 Mb/s. Station  $B$  responds with a 14 octet acknowledgment also at 5.5 Mb/s. In the figure  $t_{tx}$  represents the time when the first symbol of the data frame is transmitted and  $t_{rx}$  the time when the first symbol of the ACK frame is received. The round-trip time  $t_{rtt}$  is computed as shown in equation 1:

$$t_{rtt} = t_{rx} - t_{tx} - t_p \quad (1)$$

Where the term  $t_p$  denotes the total time to transmit the data frame which, in this example, is  $283\mu\text{s}$ . The value of  $t_p$  is given by the TXTIME calculations of the IEEE 802.11 specification and depends on the PHY layer encoding, the transmission rate, frame size and whether short or long preambles are being used [7]. After receiving the data frame station  $B$  waits for a SIFS period before transmitting the ACK frame. To determine the actual two-way TOA  $t_a$  this SIFS period must be adjusted for as shown in equation 2.

$$t_a = t_{rtt} - SIFS \quad (2)$$

From the two-way TOA  $t_a$  we can derive an estimate of the distance to the target station as shown in equation 3.

$$d = v \frac{t_a}{2} \quad (3)$$

Where  $d$  is the distance in meters,  $v$  is the velocity of a radio wave through the air ( $\approx 2.998 \times 10^8$  m/s) and  $t_a$  the two-way TOA in seconds.

## B. Outline of the paper

The rest of this paper is organized as follows. The proposed distance-ranging attack is described in the next section. A brief survey of related work is given in Section III. Section IV describes the experiments and Section V presents an analysis of the results. We present our conclusions in section VI.

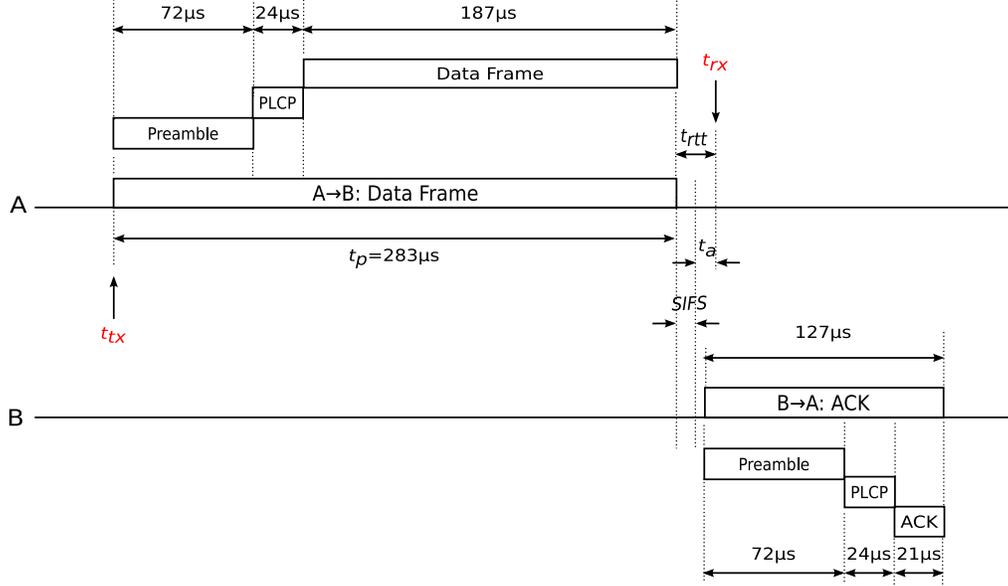


Fig. 1. Example timing diagram for an IEEE 802.11 DATA/ACK exchange.

## II. PROPOSED DISTANCE-RANGING ATTACK

The goal of an attack against the distance-ranging procedure is to allow the attacker to misrepresent the reported distance to appear either much further away or much closer than they really are. The flaw that makes an attack possible is the presumption of a non-adversarial situation. The two-way TOA distance-ranging procedure requires the cooperation of the target station to make an accurate TOA measurement. In an adversarial setting the adversary need adjust their SIFS value to advance or delay transmission of the ACK. If the adversary adjusts the SIFS period by  $\delta\mu\text{s}$  then the effective distance ranging equation is as shown in equation 4:

$$d = v \left( \frac{t_{rx} - t_{tx} - t_p - SIFS + \delta}{2} \right) \quad (4)$$

A  $\delta$  of  $-1\mu\text{s}$  will have the effect of reducing the SIFS interval and result in a decrease in the apparent distance by almost 150m. Increasing the value of  $\delta$  by  $1\mu\text{s}$  will increase the SIFS interval and have the opposite effect. The proposed attack is not specific to IEEE 802.11 but is general and applies to other wireless technologies where two-way TOA distance-ranging is employed. The only requirement for an adversary to subvert the two-way TOA distance-ranging procedure is that they are able to control the timing of the inter-frame spacing used by their wireless network interface controller (WNIC). The implementation of the proposed attack is very simple. Modern WNIC designs often make use of FullMAC approaches in which the device driver is responsible for implementing the IEEE 802.11 stack. These devices expose registers that allow for extensive control over the physical layer. Where the device exposes the SIFS interval timer the driver can be modified to allow  $\delta$  to be applied to the normal SIFS value.

## III. RELATED WORK

In current-generation WNICs timestamps have a resolution of  $1\mu\text{s}$  at best — many commodity WNICs have much lower timestamp resolution and are thus unsuitable for estimating distance. As a result Günther and Hoene take multiple two-way TOA measurements at a resolution of  $1\mu\text{s}$  and employ statistical post-processing to arrive at a location accuracy to within 5m [4]. A similar approach using different statistical techniques has also been adopted by Ciurana, *et al.* [6]. The need to do hundreds of measurements limits the real-world applicability of the approach so several researchers have investigated the use of higher-resolution timestamps not normally available in commodity hardware. In other work Ciurana *et al.* adopted a software-based approach using the Intel Pentium’s Time Stamp Counter (TSC) timing register which increments at the CPU clock frequency but is subject to the latencies and vagaries of interrupt scheduling [8]. Izquierdo *et al.* made use of customized hardware to obtain timestamps from the WNIC’s 44MHz internal clock combined although still required statistical post-processing of multiple readings [9]. Golden and Bateman also used customized WNIC hardware and identified significant variations in the time taken for different WNICs to generate acknowledgements [3]. Instead of replying immediately after the SIFS interval it was found that in many WNICs an additional time delay of several microseconds is incurred. These “MAC processing” delays are so large that two-way TOA distance ranging is not possible without being able to adjust for the delay. The proposed IEEE 802.11v standards amendment adds a Timing Measurement Frame (TMF) that allows stations to discover and adjust for this additional delay and also eliminate the need for multiple readings to obtain an accurate TOA [10].

These MAC processing delays represent ranging errors of hundreds of meters precision and this motivated the spec-

ification of the TMF to enable the use of two-way TOA distance-ranging. The TOA approaches above have been extended by Hoene and Willmann to a *four-way* TOA distance-ranging procedure which is used in the GoodTry localization procedure [5]. This scheme uses a RTS/CTS/DATA/ACK exchange as the basis for its measurements and this has the advantage that both stations can determine a distance as well as allowing third parties to estimate the distance between the participating stations. As with the two-way procedure the four-way approach also relies on the honest participation of the target station and so is also subject to the proposed attack described here.

A cryptographic protocol for distance-bounding has been proposed by Brands and Chaum [11] and applied to wireless networks by Čapkun *et al.* [12]. Distance-bounding protocols seek to fix a bound on the distance between legitimate parties using precise timing of a rapid bit exchange used as part of a cryptographic bit-commitment protocol. With such a protocol the adversary can pretend to be further away than they are in reality but can never appear to be closer. Distance-bounding protocols demand a low-latency, low-noise, high-speed communications channel optimized for single bit exchanges. The application of cryptographic distance-bounding protocols to wireless environments appear promising but the security of the mechanism depends critically on the details of the implementation. IEEE 802.11 and similar wireless networks are unsuitable because of the relatively noisy and high-latency communication channel which does not support the requirements for rapid bit exchange [13]. Hancke and Kuhn have demonstrated how simple attacks can substantially undermine these approaches and identify the need for special hardware support for wireless bit-commitment protocols [14]

#### IV. EXPERIMENTS

This section describes the equipment, configuration and method used to conduct the experimental evaluation.

##### A. Equipment

The equipment used consists of a wireless mesh router, a wireless mesh client and two monitoring stations as shown in figure 2. The wireless mesh router is a dedicated device equipped with a 1.6 GHz AMD Sempron processor and two IEEE 802.11abg WNICs using the the Atheros AR5213A chipset. The wireless mesh client is equipped with a single IEEE 802.11bg WNIC which also using the Atheros AR5213A chipset. Data is collected at the monitoring stations. The first of these is an IBM T22 laptop with an IEEE 802.11b WNIC based on the Intersil PRISM II chipset. This interface is intended solely for data collection and has been chosen because of its receive sensitivity and ability to collect traffic with timestamps with a documented resolution of  $1\mu s$ . The second monitoring station is a Lenovo T61p laptop is used with an Atheros AR5213A-based WNIC. Collecting data from two different WNICs based on different chipsets is intended to compensate for capture errors which may occur because of errors in the WNIC or device driver. All of the WNICs used in the experiments make use of external low-gain (approx 5dB) antennas which are omni-directional in the horizontal plane.

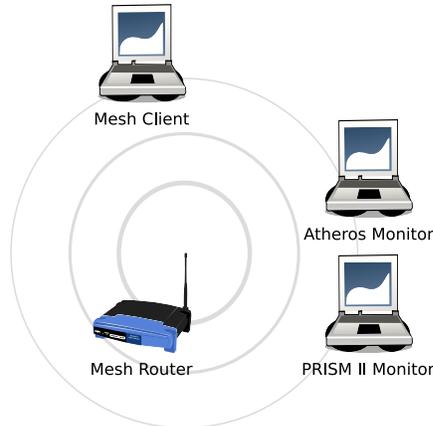


Fig. 2. Laboratory equipment

##### B. Configuration

All of the computers used in the experiments use the GNU/Linux operating system. Both the wireless mesh router and the wireless mesh client run a custom build of the Linux kernel version 2.6.30.4 in which support for mesh networking conforming to the the draft IEEE 802.11s standard has been enabled. This kernel also has a modified version of the `ath5k` device driver which allows the hardware SIFS time to be adjusted using the `sysfs` filesystem and which is restricted to operate to 802.11b mode. The latter modification is required so that data can be captured using the PRISM II-based WNIC which is capable only of 802.11b operation.

1) *Mesh router/client changes:* The AR5213 devices are capable of operating in a variety of transmission and reception modes. The `ath5k` device driver does not allow a specific hardware mode to be selected and so the device driver initialization has been modified to restrict the operation to 802.11b mode during the device initialization when selected by a module parameter. Changing the mode dynamically is possible but there are a large number of ancillary data structures which also need modifying. A change to the initialization routine has the least impact on other functions within the driver. The SIFS is more easily changed and the `sysfs` service routines simply change the appropriate WNIC register. In normal operation the WNIC was observed to experience frequent hardware resets that would cause this setting to be lost. In order to preserve the SIFS value across hardware resets its value is also changed in the table of initial register values that are written to the WNIC during a reset.

2) *Monitoring station changes:* The T22 monitoring station makes use of the HostAP device driver for the PRISM II WNIC. The T61 can dual-boot to run either Linux kernel 2.6.24 or 2.6.30.4 to be used. In the former configuration the `MadWiFi-NG` device driver is used; in the latter this has been superseded by the `ath5k` device driver. The `ath5k` device driver is modified to restrict operations to 802.11b mode in exactly the same was as for the mesh router and client stations.

### C. Experimental Method

The mesh stations and monitors are all located in the same lab setting and within 3m of each other to minimize the actual time-of-flight and multi-path effects. The mesh stations establish a link and enable RTS/CTS protection to minimize interference from neighboring networks. Both the mesh router and the mesh client are capable of performing the distance-ranging procedure but for the purpose of the experiment it is the wireless mesh router that is used as the ranging station and the wireless mesh client the target. Data traffic is generated using `iperf` program [15]. Data collection takes place at the monitoring stations using the `tcpdump` packet sniffer [16]. Frames are captured in monitor mode (i.e. promiscuous capture of all frames received by the interface) in which every frame is prefixed with a header which provides information about the received frame. This information includes the timestamp, data rate and the received signal strength and noise values.

1) *Timestamp Calibration*: The WNIC devices used in this experiment are all based on the Atheros AR5213A chipset. There is no documentation publicly available detailing the resolution of the timestamps produced by these devices. There is some concern over the timestamp accuracy simply because it is undocumented. A further cause for concern is in because the device attaches a 16 bit timestamp to the received frame’s descriptor and this is extended by the device driver into a 64 bit value. This extension occurs in the interrupt service routine with MadWiFi-NG doing the TSF extension in the *top-half* of the interrupt service routine and `ath5k` deferring this to the *bottom-half*. The difference in the strategy for TSF-extension of the hardware timer is important because of the structure of the device driver’s interrupt service routine. It is the job of the top-half to respond immediately to the cause of the interrupt whereas the bottom half is less time critical and so the device driver defers this for later execution. If the delay is significant then the probability that the TSF extension may be incorrect is increased.

To verify the accuracy and resolution of the timestamps a simple experiment captures traffic between the two mesh stations using the PRISM II based WNIC and an Atheros 5313A based WNIC. A single 30 second exchange of bi-directional UDP data is generated between mesh client and mesh router using the `iperf` program and captured by the two monitors. The experiment is conducted first using the MadWiFi-NG device driver and then repeated using `ath5k`.

2) *SIFS Modification*: To determine the effectiveness of the proposed attack `iperf` is used to generate bi-directional UDP traffic at a rate of 1 Mb/s across this link for a period of 2 minutes. Special “marker” frames are injected immediately before and after each `iperf` test to assist in correlating the results from different WNICs. This test is repeated for SIFS values of between 0 – 29 $\mu$ s in 1 $\mu$ s increments. The mandated value of the SIFS in IEEE 802.11b is 10 $\mu$ s and the maximum is given by the PIFS value (which is 30 $\mu$ s). Thus the range of values under test covers the range of possible SIFS values for IEEE 802.11b.

### V. ANALYSIS OF RESULTS

Accurate timing is essential for the successful operation of the two-way TOA ranging procedure and gauging the practicality of the proposed attack. In this section we discuss the results in two parts. The first concerns the time measurement results which will be of relevance to those considering the use of two-way TOA distance ranging. The second part discusses those findings particular to the attack itself.

#### A. Timing Measurement

There is a difference between the timestamps reported by the different WNICs in that the PRISM II WNIC timestamp marks the arrival of the first symbol of the frame at the receiver whereas the Atheros AR5213 attaches a timestamp which is taken at a point near the end of the frame. When this is accounted for the results returned from MadWiFi-NG are closely correlated with those for the PRISM II WNIC as shown in table I. The row marked “Filtered” in the table refers to results which have been filtered out of the analysis. The section below on Jumping Timestamps addresses the reason why this particular value has been excluded.

TABLE I  
TIMING CALIBRATION RESULTS

	Number of Data/ACK Frames	Number of Filtered Frames	SIFS ( $\mu$ s)		
			Min	Max	Avg
MadWifi-NG	4263	1	10	11	10.55
PRISM II	4223	0	9	23	10.56
<code>ath5k</code>	4176	0	1	425985	214.77
PRISM II	4265	0	9	11	10.5

1) *“Jumping” timestamps*: We have observed that occasionally the timestamp reported by MadWiFi-NG appears to jump by as much as 70ms between successive frames in an atomic RTS/CTS/DATA/ACK exchange. This has the effect of making it seem that an extremely long time has elapsed between successive frames. The reason for concluding this is not what has actually happened is because it is not consistent with either the PRISM II capture or with the IEEE 802.11 Network Allocation Vector (NAV) and that despite a supposed 70ms delay there is no other intervening network traffic (e.g. beacons).

The NAV is a useful for resolving these problems because it provides information with a resolution of 1 $\mu$ s and is essential for the successful operation of an IEEE 802.11 network. The NAV is specified in frame header and used to reserve the channel for an upcoming exchange and all stations overhearing the NAV will wait for the reservation to expire before transmitting. In a four-way exchange the NAV is set by the RTS to the time needed for the remainder of the exchange. In a two-way exchange it is set by the DATA frame. The subsequent frames in the exchange adjust this value to reflect elapsed time. Using the NAV it is possible to obtain relative timestamps and TXTIMES for the CTS, DATA and ACK components of the four-way exchange or for the ACK component of a two-way exchange. Thus we can compare against both WNIC and the NAV to identify whether it is the `ath5k` or PRISM II timestamps which are in error.

In this case the NAV allows us to conclude that it is MadWiFi-NG that is providing incorrect timestamps. This has been accounted for in table I where a single four-way exchange contains such a jumping timestamp and has been filtered from the results. The same filtering process has been applied also to the SIFS variation experiments. Where the timestamp jumps the value is always in the range 65-75ms and this is suspiciously close to the 65ms which could arise from a bug in the TSF extension logic.

2) *Bad timestamps*: The second set of results in table I compares the ath5k and PRISM II results. The ath5k results are computed in exactly the same manner as for MadWiFi-NG and the summary shows the extreme nature of the results. There is a single instance in the capture file where the timestamp suggest a SIFS of 425ms and the frequency distribution of SIFS is otherwise bi-modal with the SIFS values being reported as either  $1\mu\text{s}$  or  $63\mu\text{s}$ . These timestamps assume values that are quite incompatible with those from the PRISM II WNIC or the NAV. In the case of the ACK frame indicating a 425ms difference between itself and the preceding frame the NAV indicates that the actual time taken to transmit the DATA is  $12474\mu\text{s}$ — which is the the same as the PRISM II card timestamp reports for the DATA + SIFS. So, both NAV and PRISM agree and there is also no intervening traffic and this is, therefore, presumed to be an analogous problem to that of the MadWiFi-NG jumping timestamp. In the present configuration ath5k is producing timestamps of much lower resolution than MadWiFi-NG and these are unsuitable for two-way TOA distance-ranging. The fact that MadWiFi-NG produces accurate timestamps suggests this is merely a software problem and that a suitable bug-fix will remedy the situation.

3) *Bad frame sizes*: Problems were experienced in the packet sniffer captures relating to the received frame length. This is a cause for concern because it may result in incorrectly-computed TXTIME calculations which directly affect the accuracy of the two-way TOA distance-ranging procedure. The problems found with the captured data are that:

- PRISM II captures contain control frames which are sometimes not properly truncated. Such frames are often very large and filled with garbage from previous frame contents.
- MadWiFi-NG captures control frames which are truncated prematurely. In this case they are missing the last two octets of the frame (thus the frame checksum (FCS) which falls at the end of the frame is partially missing).

In both cases these problems appear to affect only the fixed-length control frames RTS, CTS and ACK. The problem has not been observed for DATA frames which are variable-sized but which `iperf` ensures are filled to the maximum of 1534 octets. When capturing with MadWiFi-NG all of the control frames are truncated by two octets which is confirmed by viewing the packet captures in the `Wireshark` protocol analyzer. The same frames are present in both PRISM II and MadWiFi-NG captures suggesting this is a simple driver bug. An analysis of the NAV values finds that the estimated TXTIME and NAV agree only when the missing two octets are considered as part of the frame. A comparison with the

TABLE II  
FREQUENCY OF INCORRECT FRAME SIZES CAPTURED BY PRISM II

RTS		CTS		ACK	
Size (Octets)	Freq	Size (Octets)	Freq	Size (Octets)	Freq
24	3	18	4	18	2
42	2	36	1	41	94
47	183	41	151	78	2
52	3	46	3	80	2
62	1	78	4	86	1
84	2	80	1	90	33
90	1	84	1	134	4
92	4	86	4	1516	295
96	46	90	49		
140	7	134	4		
784	2	778	2		
1522	550	1516	432		
	804		656		403

ath5k captures shows that the control frames are received without truncation. We conclude, therefore, that this is simply a bug in the MadWiFi-NG device driver and adjust truncated frame lengths accordingly.

The problem with the PRISM II WNIC results in frames being returned to the packet sniffer which are much larger than were transmitted over the air. A summary of the bad frame sizes captured across all of the timestamp calibration experiments is give in table II. For these experiments the PRISM II WNIC successfully captured 17008 four-way exchanges of which 1608 contained one or more incorrectly-sized frames. Truncation errors often results in the frame size growing by two orders of magnitude to over 1500 octets.

The frame length errors described above can be compensated for in software. The PRISM II WNIC timestamps the frame beginning and so computes the TXTIME for a data frame — which have not been found to be in error. The AR 5213 timestamps the end of the frame and so needs to compute the TXTIME for the ACK but this does not pose any problem because the same two octet adjustment can be made for all ACK frames.

### B. TOA Measurement

In section III we discussed the approaches used to take the raw timing information and use it for two-way TOA measurement. This section re-visits some of these topics in the light of the experience gained from the experiments.

1) *Software-based approaches*: The Intel Pentium supports a timestamp counter (TSC) which is incremented at the rate of the CPU clock. Günther and Hoene considered using this timer but rejected it because of presumed interrupt latencies [4]. Nonetheless the approach has been pursued by Ciurana *et al.* [8] with some success. In principle the TSC value could be read and stored in the interrupt vector and would allow the measurement of the intervals between interrupts with only the bus latency and interrupt priority to consider. The main problem is interrupt priorities but these could be handled by careful design of the interrupt handler or the adoption of a nano-kernel approaches. In the experimental testbed the ath5k driver has been instrumented to allow the use of the

processor's TSC but the problems in obtaining accurate results from the hardware has meant deferring experimental analysis. Future work should compare careful design to reduce the latencies associated with interrupt handling with the nano-kernel approach. A nano-kernel achieves real-time handling of interrupts in ring 0 whilst the operating system kernel occupies ring 1 and has interrupts dispatched to it via the nano-kernel. This allows the separation of interrupt response and dispatch - reducing latencies still further. We intend to further investigate the use of the TSC for time-stamping although there are other potential problems. In multi-core CPUs the same TSC is shared between all cores whereas in multi-processor environments each processor may have its own TSC. Using TSC for time-stamping in such environments presents further challenges.

2) *Acknowledgment Timing Variations*: The results of the SIFS variation experiment are shown in figure 3 which plots the expected against observed SIFS times on the link under test using data collected from the MadWiFi-NG device driver. A total of 573 DATA/ACK exchanges have been filtered from the results because they were deemed to be jumping timestamps from a total of 663349 DATA/ACK exchanges — just 0.086% of the total exchanges.

From the graph it is clear that observed SIFS timings are on average between  $2-3\mu\text{s}$  greater than the expected SIFS time. It is also clear that the SIFS timer can be reduced below the expected SIFS value. In the chart the lowest average setting that is achieved is  $6.75\mu\text{s}$ . This is significant because it represents a decrease of  $5.25\mu\text{s}$  from the time the card would normally take to produce the SIFS. This means that a hostile adversary can appear to be about 750m *closer* to their target as well as significantly further away. Below a SIFS setting of  $4\mu\text{s}$  there appears to be no further reduction in SIFS time. There is a minimum time required to switch between receive and transmit for this WNIC and for this WNIC it appears to be approximately  $4\mu\text{s}$ .

Golden and Bateman also report that there can be considerable variation in the time taken to generate acknowledgments for different WNIC designs [3]. In the hardware under test the SIFS appeared to be generated  $2-3\mu\text{s}$  after the SIFS period expires and this represents a possible distance error of 300-450m. So, for the hardware under test the ACK is generated in a predictable manner but with the possibility of a significant additional delay that can dwarf the distance between ranging and target station.

Stratigakis [17] has a patent to ensure that WNIC MAC controllers do not waste substantial resources in timing loops and ensure that ACKs are generated immediately the SIFS timeout occurs. This makes use of hardware-based timers and the patent has been assigned to Cisco. The alternative approach has been advocated by Golden [18] and later adopted in the IEEE 802.11v draft standard which defines the TMF to enable allow ranging stations to discover, and adjust for, any the additional MAC processing delays present in the hardware of the target station.

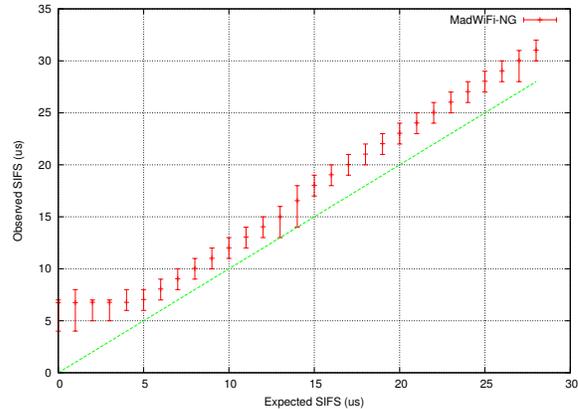


Fig. 3. Expected and observed SIFS times

### C. Security of Two-Way TOA Distance Ranging

The experiments demonstrate that the attack is effective and will allow a station to misrepresent its position to a substantial degree. It is, therefore, essential to understand the risk model and how it is affected by this attack. There are two separate threats which must be considered:

- The first is where a hostile adversary is misrepresenting their own position. Such an approach maybe used, for example, to subvert location-based authentication or a localization procedure designed to monitor network stations' physical locations.
- The second threat is more subtle and involves an adversary who wishes to misrepresent the location of another station. Such an adversary maybe conducting a worm-hole or man-in-the-middle attack aimed at subverting the routing, authentication or other higher-layer protocols.

The necessary condition for the secure use of two-way TOA distance-ranging is that the target of the distance-ranging procedure behave honestly. This is clearly not the case when the target station is under the control of a hostile adversary and so this procedure cannot be used for location-based authentication and secure localization. The sufficient condition for the secure use of two-way TOA procedure is that the time-bounded round-trip measurement is for the the exchange of messages between the honest parties and the whole exchange is authentic and timely. If, and only if, both these conditions are satisfied can the results of the two-way TOA procedure be considered trustworthy.

In IEEE 802.11 the latter condition does not hold because there is no provision for authenticating ACKs. A man-in-the-middle or wormhole attack can generate its own ACKs to precisely control the timing of the acknowledgments. IEEE 802.11v has introduced the TMF specifically to support two-way TOA distance-ranging but this also presumes a non-adversarial setting. The TMF frame itself is not protected by the security protocol and is sent in the plain. This means that the adjustment value may be modified by an attacker conducting a man-in-the-middle or wormhole attack to misrepresent the distance to the target station.

Authenticating the acknowledgment is a desirable defense against the man-in-the-middle and wormhole attack because it forces the adversary to relay all the message traffic between stations. In this case the additional latency of the the round-trip time would expose the presence of the man-in-the-middle or wormhole. The adversary is still able to further delay the return message but this would make the apparent distance larger again and expose the adversary's presence. An additional benefit of authenticating acknowledgments is that it affords no possibility to the attacker for message re-ordering or deletion without that re-ordering or deletion being discovered by the sender. Such a scheme is being investigated as further work in which a modified MAC protocol is used to ensure authenticity of the ACK. The limitation of such a proposal is that distance-ranging can only be established for frames which are part of a secure association at the link-layer.

## VI. CONCLUSIONS

The contribution of this paper consists of several parts. Firstly, we have identified the attack and demonstrated its practicality. Secondly, we have identified both the capabilities and limitations of commercially available hardware with regard to this attack and the capture of precise timing information. Thirdly the paper clearly identifies the limits of trustworthiness of distance estimates arrived at by the two-way and four-way TOA procedures. Finally, a countermeasure is suggested to the important man-in-the-middle/wormhole attack scenario.

The two-way TOA distance-ranging procedure is insecure because it assumes a non-adversarial setting and requires the honest cooperation of a potential adversary. In the case of IEEE 802.11 and similar wireless networks the adversary can subvert the distance-ranging procedure and vary this time significantly to appear to be either closer or further away than they are in reality. Thus, we conclude that two-way and four-way TOA distance-ranging are not suitable for use as a security primitive in wireless networks.

## ACKNOWLEDGMENTS

NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Center of Excellence program; and the Queensland Government.

## REFERENCES

- [1] Dennis D. McCrady, Lawrence Doyle, Howard Forstrom, Timothy Dempsey, and Marc Martorana. Mobile ranging using low-accuracy clocks. *IEEE Transactions on Microwave Theory and Techniques*, 48(6):951–958, June 2000.
- [2] Harish Reddy, M.Girish Chandra, P. Balamuralidhar, S.G. Harihara, Kaushik Bhattacharya, and Edward Joseph. An improved time-of-arrival estimation for WLAN-based local positioning. In *2nd International Conference on Communication Systems Software and Middleware (COMSWARE 2007)*, pages 1–5, January 2007.
- [3] Stuart A. Golden and Steve S. Bateman. Sensor measurements for Wi-Fi location with emphasis on time-of-arrival ranging. *IEEE Transactions on Mobile Computing*, 6(10):1185–1198, 2007.
- [4] André Günther and Christian Hoene. Measuring round trip times to determine the distance between WLAN nodes. *Lecture Notes in Computer Science*, 3462:768–779, January 2005.
- [5] Christian Hoene and Jörg Willmann. Four-way TOA and software-based trilateration of IEEE 802.11 devices. In *IEEE 19th International Symposium Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*, pages 1–6, September 2008.
- [6] Marc Ciurana, Francisco Barceló-Arroyo, and Sebastiano Cugno. A robust to multi-path ranging technique over IEEE 802.11 networks. *Wireless Networks*, pages 1–11, April 2009.
- [7] LAN/MAN Standards Committee of the IEEE Computer Society. *IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 802.11-2007 edition, June 2007.
- [8] Marc Ciurana, David López, and Francisco Barceló-Arroyo. SofTOA: Software ranging for TOA-based positioning of WLAN terminals. In *Proceedings of 4th International Symposium on Location and Context Awareness (LoCA 2009)*, volume 5561/2009 of *Lecture Notes in Computer Science*, pages 207–221, Tokyo, Japan, May 2009. Springer Berlin / Heidelberg.
- [9] Fernán Izquierdo, Marc Ciurana, Francisco Barceló, Josep Paradells, and Enrico Zola. Performance evaluation of a TOA-based trilateration method to locate terminals in WLAN. In *1st International Symposium on Wireless Pervasive Computing*, pages 1–6, Jan. 2006.
- [10] LAN/MAN Standards Committee of the IEEE Computer Society. *IEEE P802.11v™/D7.0 Draft standard for information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 8: Wireless Network Management*, July 2009.
- [11] Stefan Brands and David Chaum. Distance-bounding protocols. In *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptography*, pages 344–359, Secaucus, NJ, USA, 1993. Springer-Verlag New York, Inc.
- [12] Srđan Čapkun, Levente Buttyán, and Jean-Pierre Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 21–32, New York, NY, USA, 2003. ACM Press.
- [13] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore. So near and yet so far: distance-bounding attacks in wireless networks. In Levente Buttyán, Virgil D. Gligor, and Dirk Westhoff, editors, *ESAS*, volume 4357 of *Lecture Notes in Computer Science*, pages 83–97. Springer, 20–21 September 2006.
- [14] Gerhard P. Hancke and Markus G. Kuhn. Attacks on time-of-flight distance bounding channels. In *WiSec '08: Proceedings of the first ACM conference on wireless network security*, pages 194–202, New York, NY, USA, 2008. ACM.
- [15] `iperf` network testing tool. Webpage. <http://sourceforge.net/projects/iperf>.
- [16] `tcpdump` packet analyzer. Webpage. <http://www.tcpdump.org>.
- [17] John Stratigakis. Hardware assist system and method for the timing of packets in a wireless network. US Patent 7233588, US Patent Office, June 2007.
- [18] Stuart Golden. Usage of timestamps in WLAN for localization and other applications. IEEE 802.11 Working Group Document 05/0161r0, Institution of Electrical and Electronics Engineers, March 2005. Available from <https://mentor.ieee.org/802.11/dcn/05/11-05-0161-00-0wng-usage-timestamps-in-wlan.ppt>.